

# **INFORMATIEBEVEILIGING EN GEMMA**



## Colofon

### Naam document

informatiebeveiliging en GEMMA.

### Versienummer

1.0

### Versiedatum

Mei 2016

### Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

### Copyright

© 2016 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. Het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;
4. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

### Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

### Doel

Het doel van dit document is om beveiligingsdoelen, principes en eisen van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) aan Gemeentelijke Model Architectuur (GEMMA) te relateren.

### Doelgroep

Dit document is van belang voor iedereen die zich bezig houdt met GEMMA: van gemeenteambtenaren tot leveranciers tot medewerkers van KING.

## Inhoud

<b>i. Versiebeheer/Wijzigingshistorie</b>	<b>4</b>
<b>1 Inleiding</b>	<b>5</b>
Doel van het document	5
Leeswijzer	5
<b>2. Baseline Informatiebeveiliging Nederlandse Gemeenten</b>	<b>6</b>
2.1 Inleiding	6
2.2 Baseline Informatiebeveiliging Nederlandse Gemeenten	6
2.3 Uitgangspunten BIG	7
2.4 Informatiebeveiliging in een gemeente	8
<b>3. GEMMA 2</b>	<b>11</b>
3.1 Inleiding	11
3.2 Opbouw GEMMA 2	11
3.3 Architectuurprincipes	11
3.4 Soorten architecturen	14
3.4.3 Overige architectuurmodellen	18
<b>4. Informatiebeveiliging in GEMMA 2</b>	<b>19</b>
4.1 Inleiding	19
4.2 Positionering informatiebeveiliging binnen GEMMA 2	19
4.3 Bedrijfsarchitectuur	20
4.3.1 Sturing	21
4.3.2 Ontwikkeling	22
4.3.3. Bewaking	23
4.3.4 Regievoering	25
4.3.5 Klant - en keteninteractie	26
4.3.6 Beoordeling	27
4.3.7 Uitvoering	27
4.3.8 Ondersteuning	28
4.4 Procesarchitectuur	28
4.5 Informatiearchitectuur	30
4.5.1 Functionaliteit voor burgers/bedrijven	31
4.5.2 Functionaliteit voor gemeente	33
4.5.3 Platformfunctionaliteit	40

### Bijlage 1: Literatuur/bronnen

Fout! Bladwijzer niet gedefinieerd.

## **i.   Versiebeheer/Wijzigingshistorie**

Hier worden de wijzigingen op dit document beschreven die zijn goedgekeurd en door wie.

### **Versies**

<b>Versie</b>	<b>Datum</b>	<b>Auteurs</b>	<b>Samenvatting van de wijzigingen</b>
0.1	22 juni 2015	John van Huijgevoort	Initieel document
0.4	20 augustus 2015	John van Huijgevoort	Opmerkingen van de Architectuurboard verwerkt.
0.5	Januari 2016	Laurens van Nes	
0.6	April 2016	J. Hintzbergen	Review, aanpassingen

### **Goedkeuring**

<b>Versie</b>	<b>Datum</b>	<b>Naam</b>

## **1 Inleiding**

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties ook voor gemeenten van groot belang. Burgers, ketenpartners en bedrijven verwachten een goed functionerende, dienstverlenende gemeente. Samenwerking tussen gemeenten onderling, maar ook een betrouwbare communicatie met ketenpartners en bedrijfsleven zijn hiervoor belangrijke voorwaarden. GEMMA, de Gemeentelijke Model Architectuur, maakt deze samenwerking en de daarvoor benodigde interoperabiliteit mogelijk vanwege een op dezelfde leest geschoeide architectuur. Informatiebeveiliging is een belangrijk onderdeel van het waarborgen van een betrouwbare, beschikbare en correcte informatiehuishouding van gemeenten. Informatiebeveiliging is het proces dat deze betrouwbare informatievoorziening borgt en is opgenomen als een kwaliteitscriterium van de bedrijfsvoering.

In dit document worden onderdelen van de Gemeentelijke Model Architectuur verbonden aan het gemeentelijke normenkader voor informatiebeveiliging, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

### **Doel van het document**

Dit document heeft tot doel om gemeenten te informeren over de informatiebeveiligingsaspecten uit de integrale Baseline Informatiebeveiliging Nederlandse Gemeenten die van belang zijn bij het ontwerpen van (digitale) gemeentelijke dienstverlening. De focus ligt op die beveiligingsaspecten waarbij organisaties in hun informatieketens het meest van elkaar afhankelijk zijn.

De integrale BIG bestaat een strategische baseline, een tactisch normenkader met 11 hoofdstukken en ongeveer 300 normen, en operationele handreikingen. Geprobeerd wordt om deze hoofdstukken en normen uit de BIG zo concreet als mogelijk te verbinden en inzichtelijk te maken voor specifieke onderdelen uit de GEMMA 2. De onderdelen zijn het bedrijfsfunctiemodel, de informatiearchitectuur en de procesarchitectuur.

### **Leeswijzer**

In hoofdstuk 2 is de integrale Baseline Informatiebeveiliging Nederlandse Gemeenten beschreven (BIG). Er is aandacht voor de opzet, de documenten, uitgangspunten en de inrichting van de BIG in een gemeente. In hoofdstuk 3 is kort de opbouw, principes en de architectuurlagen van de GEMMA 2 toegelicht. In hoofdstuk 4 wordt de verbinding tussen informatiebeveiliging en de GEMMA 2 gepresenteerd.

## **2. Baseline Informatiebeveiliging Nederlandse Gemeenten**

### **2.1 Inleiding**

In dit hoofdstuk wordt de BIG kort toegelicht. In paragraaf 2.2 is de opzet van de BIG vanuit toegelicht. Paragraaf 2.3 beschrijft de uitgangspunten van de BIG. Paragraaf 2.3 gaat over de inrichting van de gemeentelijke informatiebeveiliging vanuit de BIG. Deze inrichting van de informatiebeveiliging is zeker in het geval van nieuwe ontwikkelingen of projecten belangrijk. Bij nieuwe ontwikkelen of project moet namelijk altijd een baselinetoets en eventueel een diepgaande risicoanalyse worden uitgevoerd.

### **2.2 Baseline Informatiebeveiliging Nederlandse Gemeenten**

#### **Informatiebeveiliging**

Het werkgebied van de BIG omvat de bedrijfsvoeringsprocessen, onderliggende informatiesystemen en informatie van de gemeente in de meest brede zin van het woord. De BIG is van toepassing op alle ruimten van een gemeentehuis en aanverwante gebouwen. Alsmede op de apparatuur die door gemeente ambtenaren gebruikt worden bij de uitoefening van hun taak op diverse locaties. De BIG heeft betrekking op de informatie die daarbinnen verwerkt wordt. Als informatiesystemen niet fysiek binnen de gemeente draaien is de BIG Strategische ook van toepassing.

- Personele veiligheid en integriteit: de veiligheid voor medewerkers en bezoekers van een organisatie en de invulling van de begrippen "goed burgerschap" en "goed werkgeverschap";
- Fysieke beveiliging: de veiligheid geboden door inrichting van gebouwen en terreinen;
- Informatiebeveiliging: de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie en verwerking daarvan (zowel handmatig als geautomatiseerd);
- Bedrijfscontinuïteit: het omgaan met risico's die een ongestoorde bedrijfsvoering bedreigen.

Informatiebeveiliging heeft daarnaast veel raakvlakken met **Risicomanagement**

Risicomanagement is het systematisch opzetten, uitvoeren en bewaken van acties om risico's te identificeren, te prioriteren, te analyseren en voor deze risico's oplossingen te bedenken, te selecteren en uit te voeren.

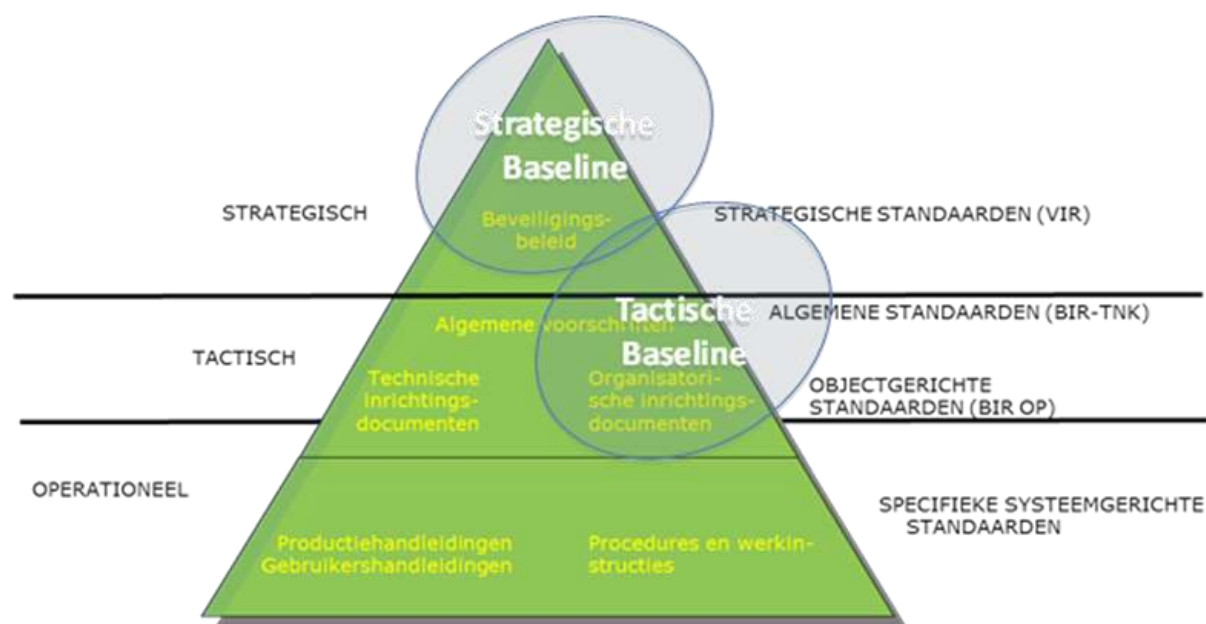
#### **Integrale Baseline bestaat uit drie delen**

Een van de overheidskaders is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Deze integrale BIG bestaat uit drie (3) delen:

1. BIG – Strategische Baseline
2. De Strategische Baseline kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. BIG – Tactische Baseline  
De Tactische Baseline beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor de gemeenten.
3. BIG – Operationele Baseline

Op basis van de strategische en tactische variant van de BIG worden operationele producten behorend bij de BIG ontwikkeld. Met behulp van deze operationele producten kan iedere gemeente tot implementatie van de BIG overgaan. Deze Operationele Baseline ondersteunen gemeenten maximaal bij het implementeren van de Strategische en Tactische Baseline.

Er is gekozen voor een optimale aansluiting bij de wereld van geaccepteerde standaarden, ISO 27001 en ISO 27002 (zie kader beveiligingsstandaarden) en de daarvan afgeleide overheidsstandaarden zoals de Voorschrift Informatiebeveiliging Rijksdienst (VIR) en Baseline Informatiebeveiliging Rijksdienst (BIR)<sup>1</sup> (zie figuur 1).



**Figuur 1 Positionering Strategische en Tactische Baseline**

## 2.3 Uitgangspunten BIG

### Basis beveiligingsniveau

BIG gaat uit van een minimumbasis beveiligingsniveau die voor veel informatiesystemen voldoende is. Voor kritieke systemen of bepaalde informatie, zoals bijzondere persoonsgegevens, biedt de BIG niet voldoende waarborgen. Door een baselinetoets uit te voeren, kan worden vastgesteld voor welke systemen of informatie dit het geval is.

Een van de voordelen van de BIG is doordat veel overheidsorganisaties gebruik maken van informatiebeveiligingsbaselines is wordt het veilig uitwisselen van informatie vereenvoudigd.

Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit en vertrouwelijkheid, waarbij vertrouwelijkheid ook soms wordt aangeduid met exclusiviteit. De BIG sluit aan bij dit onderscheid

### Beschikbaarheid

<sup>1</sup> De BIR, Baseline Informatiebeveiliging Rijk, bestaat uit BIR-TNK (tactisch normenkader) en BIR OP (Operationele baseline).

De BIG definieert een basisset aan eisen voor beschikbaarheid voor de informatie-infrastructuur van de gemeentelijke overheid. Deze dient als basis voor het maken van afspraken over de beschikbaarheid tussen de eigenaar van het informatiesysteem en de ICT-leverancier of cloud dienstverlener<sup>2</sup>. Dit houdt in dat voor de beschikbaarheid van de informatievoorziening een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden tussen de eigenaar (gebruiker) en de partij die deze beschikbaar stelt.

## **Integriteit**

Het onderwerp integriteit op ICT-vlak valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (dat wil zeggen niet gerelateerd aan het proces zelf), en de integriteit van de informatie in de applicaties of fysiek (dat wil zeggen gerelateerd aan het proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatieafhankelijk en afhankelijk van de eisen van een specifiek proces. Dit houdt in dat voor de functionele integriteit van de informatievoorziening een minimale set van normen wordt opgesteld waarbij per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

## **Vertrouwelijkheid**

De BIG beschrijft de maatregelen die nodig zijn voor het basis vertrouwelijkheidsniveau (gemeentelijk) Vertrouwelijk<sup>3</sup> en persoonsvertrouwelijke informatie zoals bedoeld in Artikel 16 van de Wet bescherming persoonsregistratie (Wbp).

## **ISO 27k en de BIG**

De ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden.

De ISO 27002 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

## **2.4 Informatiebeveiliging in een gemeente**

### **Bepalen en bewaken van de risico's en vaststellen beveiligingseisen**

Het is essentieel dat een gemeente haar beveiligingseisen bepaalt. Er zijn drie belangrijke bronnen voor beveiligingseisen:

1. de beoordeling van de risico's waar de gemeente aan blootgesteld is, rekening houdend met de algehele bedrijfsstrategie en -doelstellingen. Via een risicobeoordeling worden bedreigingen voor bedrijfsmiddelen vastgesteld, de kwetsbaarheid voor en de waarschijnlijkheid dat een bepaalde bedreiging zich voordoet, geëvalueerd en wordt de potentiële impact ingeschat;

<sup>2</sup> Denk hierbij aan Software-as-a-Service (SaaS).

<sup>3</sup> Departementaal Vertrouwelijk volgens het Besluit Voorschrift Informatiebeveiliging - Bijzondere Informatie (Vir-bi).



2. de wettelijke, statutaire, regelgevende en contractuele eisen waaraan een organisatie, haar handelspartners, leveranciers en dienstverleners, en hun sociaal-culturele omgeving, moeten voldoen;
3. de reeks van principes, doelstellingen en bedrijfseisen die gelden voor het hanteren, verwerken, bewaren, communiceren en archiveren van informatie die de gemeente heeft ontwikkeld om haar bedrijfsvoering te ondersteunen.

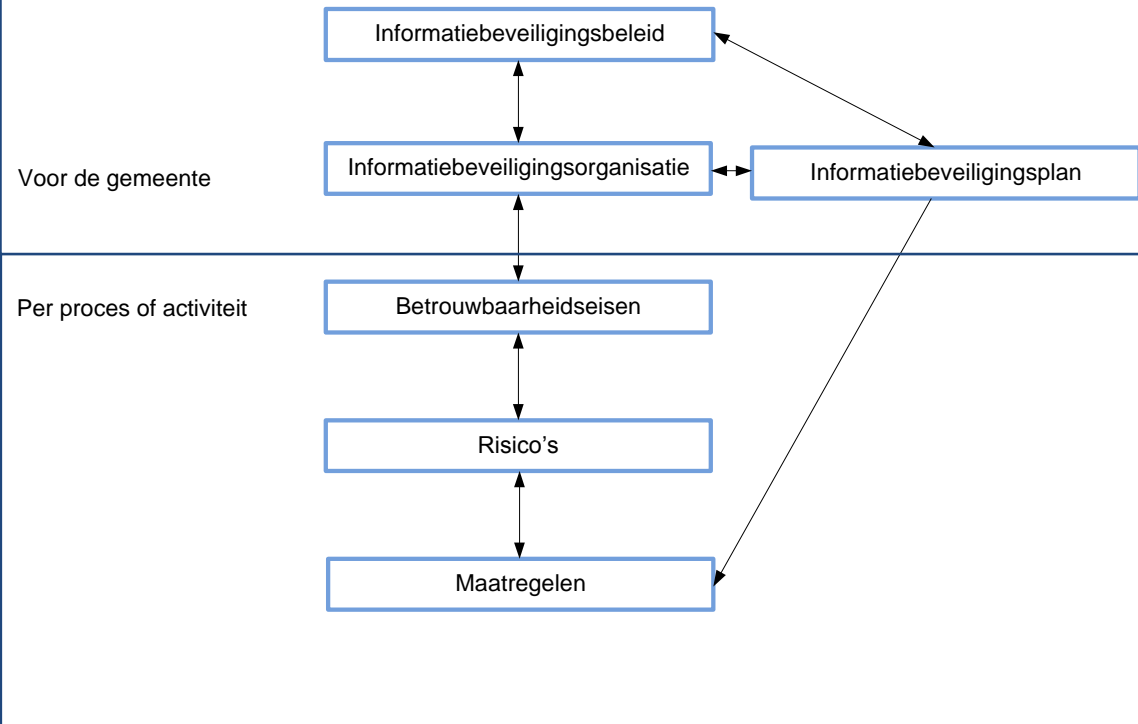
Gemeenten kunnen de BIG as is implementeren in alle processen en systemen, echter een aanpak met meer nuance help bij het selecteren van de juiste maatregelen die geïmplementeerd moeten worden, het uitvoeren van een risicoafweging is een van de mogelijkheden. De mogelijke methodes hiervoor zijn het uitvoeren van een baselinetoets BIG gevolgd door een diepgaande risicoanalyse of Privacy Impact Assessment (PIA).

Het beveiligingsniveau van BIG is zo gekozen dat dit voor de meeste processen en ondersteunende ICT-voorzieningen bij gemeenten voldoende is. Hiermee wordt voorkomen dat er voor ieder systeem een diepgaande risicoanalyse uitgevoerd moet worden. Om vast te stellen dat het niveau van deze BIG voldoende is, kan een baselinetoets BIG uitgevoerd worden. In de baselinetoets BIG wordt onder meer bekeken of er geheime of bijzondere persoonsgegevens of geclassificeerde informatie verwerkt wordt, er sprake is van persoonsvertrouwelijke informatie zoals bedoeld in artikel 16 van de Wbp, er hogere beschikbaarheidseisen vereist zijn of er dreigingen relevant zijn die niet in het dreigingsprofiel van de BIG meegenomen zijn. In deze gevallen zal een volledige risicoanalyse uitgevoerd moeten worden die kan leiden tot extra maatregelen. Bij het verwerken van (nieuwe) persoonsgegevens wordt door de uitslag van de Baselinetoets BIG ook aangeraden een Privacy Impact Assessment (PIA) uit te voeren.

Door de controle op naleving van de wettelijke voorschrift dient schending van enige wet- en regelgeving of contractuele verplichtingen, en beveiligingseisen te worden voorkomen.

Over het algemeen wordt binnen de gemeente begonnen met de BIG implementatie van de gemeentebrede maatregelen. Er zijn veel maatregelen die namelijk gemeentebreed gelden, die maatregelen hoeven dus ook niet iedere keer ingevoerd te worden. Voorbeelden hiervan zijn het maken van beveiligingsbeleid, of andere beleidsmatige maatregelen.

Er zijn binnen de BIG ook maatregelen die over het algemeen systeemspecifiek zijn, bijvoorbeeld of iets moet worden gelogd en of er gebruikersbeheer noodzakelijk is.



## **3. GEMMA 2**

### **3.1 Inleiding**

De vraag naar een architectuur voor de hele gemeentelijke informatievoorziening -dus niet uitsluitend e-dienstverlening werd steeds groter. Ook zijn de omstandigheden voor gemeenten zodanig veranderd dat de focus van de gemeentelijke organisatie sterk verbreed is, denk aan toenemende samenwerking, meer druk op de gemeentelijke financiën en de decentralisatie van een grote hoeveelheid taken in het sociaal domein. Daarnaast is er ook behoefte aan nog meer detaillering in GEMMA om het gesprek tussen en met leveranciers van de gemeentelijke informatievoorziening beter aan te kunnen gaan. Om die redenen is gestart met GEMMA 2, beginnende met de Basisgemeente en de Decentralisaties.

### **3.2 Opbouw GEMMA 2, principes en architecturen**

Architectuurprincipes zijn richtinggevende uitspraken die zorgen voor een samenhangende inrichting van de organisatie. Ze zijn een vertaling van doelstellingen, behoeften en beleidsuitgangspunten en slaan daarmee een brug naar de uitvoering.

Deze principes zijn richtinggevend en helpen gemeenten om bewust keuzes te maken bij het inrichten van de gemeentelijke processen en bijbehorende informatievoorziening. De in dit document beschreven GEMMA 2 principes verwoorden best-practices. Gemeenten kunnen zelf bepalen of zij deze adopteren. Principes zijn nadrukkelijk geen doelstellingen; ze verwoorden een algemeen streven en zeggen niets over prioriteiten. Principes zouden – net als de rest van de GEMMA referentiearchitectuur - echter niet vrijblijvend moeten zijn en er zou dan ook een proces moeten zijn waarin het maken van afwijkende keuzes expliciet wordt gemaakt. Het is aan gemeenten echter zelf om te bepalen hoe ze hier in de praktijk mee omgaan.

In de GEMMA wordt uitgegaan van drie soorten architecturen.

- Business- of bedrijfsarchitectuur. Deze bestaat uit:
  - Procesarchitectuur
  - Bedrijfsfuncties en -objecten.
- Informatiearchitectuur. Hierin wordt de informatiestrategie en de uitwerking naar concrete projecten op basis van business doelen en ontwikkelingen tot stand gebracht. Hieronder onderscheiden we ook nog twee soorten van architectuur

Applicatiearchitectuur. Gegevens- en berichtenarchitectuur

### **3.3 Architectuurprincipes**

Deze paragraaf beschrijft de GEMMA 2 architectuurprincipes die zowel de huidige ontwikkelingen als de vergezichten die op landelijk niveau worden ontwikkeld, vertalen naar een visie op de inrichting van de gemeentelijke processen en informatievoorziening.<sup>4</sup> De focus ligt hierbij op de informatievoorziening en dat is nadrukkelijk ook zichtbaar in de uitwerking van de principes. Architectuurprincipes zijn richtinggevende uitspraken die zorgen voor een samenhangende

<sup>4</sup> [http://www.gemmaonline.nl/index.php/Katern\\_GEMMA\\_Architectuurprincipes\\_compleet](http://www.gemmaonline.nl/index.php/Katern_GEMMA_Architectuurprincipes_compleet)

# INFORMATIE BEVEILIGINGS DIENST

inrichting van de organisatie. Ze zijn een vertaling van doelstellingen, behoeften en beleidsuitgangspunten en slaan daarmee een brug naar de uitvoering.



Deze architectuurprincipes zijn richtinggevend en helpen gemeenten om bewust keuzes te maken bij het inrichten van de gemeentelijke processen en bijbehorende informatievoorziening. De beschreven GEMMA 2 principes verwoorden best-practices. Gemeenten kunnen zelf bepalen of zij deze adopteren. Principes zijn nadrukkelijk geen doelstellingen; ze verwoorden een algemeen streven en zeggen niets over prioriteiten.

## 1. Onze gemeente denkt vanuit de positie van de klant

De gemeente is er voor burgers en bedrijven en zorgt ervoor dat deze de dienstverlening krijgen die ze kunnen verwachten. Zij kunnen immers niet zomaar naar een andere aanbieder als zij niet tevreden zijn. De administratieve lasten voor deze klanten moeten daarbij zoveel mogelijk worden beperkt. Klanten stellen steeds hogere eisen aan de kwaliteit van de dienstverlening van gemeenten.

## 2. Onze gemeente gebruikt generieke processen en functies

Door te denken in generieke processen en systemen kunnen diensten eenvoudiger worden gedeeld met andere gemeenten en kosten worden bespaard. Ook kan eenvoudiger gebruik worden gemaakt van standaard oplossingen die beschikbaar zijn in de markt en wordt maatwerk voorkomen. Klanten willen de overheid in haar dienstverlening ook zo veel mogelijk ervaren als één organisatie en generieke processen dragen daar aan bij."

## 3. Onze gemeente voert regie over uitbestede diensten

Gemeenten willen graag kwalitatief hoogwaardige dienstverlening bieden, maar wel tegen acceptabele kosten. De gemeente kijkt daarom kritisch of zij taken zelf uitvoert of dat het logischer is deze gezamenlijk met andere gemeenten of partners uit te voeren, of uit te besteden aan de markt. Cloud computing is een belangrijke ontwikkeling die ook als een vorm van outsourcing kan

worden gezien. Als taken elders worden belegd is het belangrijk dat de gemeente hier de regie op blijft voeren. De verantwoordelijkheid blijft namelijk bij de gemeente.

#### *4. Onze gemeente biedt de klant een goede informatiepositie*

Een goede informatiepositie is voor klanten cruciaal om snel en gemakkelijk hun weg te vinden binnen de overheid. Het zorgt er ook voor dat zij de verantwoordelijkheid kunnen nemen die in toenemende mate van hen wordt verwacht vanuit een nieuw evenwicht tussen samenleving en overheid. Dat gaat niet alleen over het ontvangen van informatie; het gaat ook over het aan het stuur zetten van de klant omtrent het gebruik van zijn gegevens. Klanten moeten in staat zijn incorrecte registratie van hun gegevens te signaleren, zodat ze voor zichzelf op kunnen komen.

#### *5. Onze gemeente digitaliseert haar diensten en processen*

Voor een modern proces is een papieren document een obstructie; het is niet efficiënt en het hindert tijd- en plaatsonafhankelijk werken. Daarom worden klanten verleid gebruik te maken van het digitale kanaal, processen zo veel als mogelijk geautomatiseerd en worden papieren documenten voorkomen. Klanten verwachten tegenwoordig ook dat dienstverlening digitaal wordt aangeboden. Dit is ook een expliciete ambitie van de overheid en uitgewerkt in de visiebrief 'Digitale overheid 2017'<sup>5</sup>. Het opslaan van gegevens in elektronische vorm maakt het veel eenvoudiger om deze te delen. Elektronische gegevens kunnen ook geautomatiseerd worden verwerkt door IT-systemen. Het elektronisch uitwisselen van gegevens is veel efficiënter en minder foutgevoelig dan het handmatig uitwisselen van gegevens.

#### *6. Onze gemeente stelt openbare gegevens als open data beschikbaar*

De overheid stelt hoge eisen aan de transparantie van overheidsorganisaties. Toegang tot informatie uit overheidsorganisaties is een kernwaarde in de democratie en is wettelijk vastgelegd. Overheidsinformatie is in beginsel vrij beschikbaar, tenzij de Wet openbaarheid van bestuur (WOB)<sup>6</sup>, Wet bescherming persoonsgegevens (Wbp)<sup>7</sup> of andere wetgeving bepaalt dat de gevraagde informatie niet geschikt is om openbaar te maken. Het openbaar, vindbaar en herbruikbaar aanbieden van open data heeft positieve maatschappelijke en economische effecten: het voorziet in een behoefte, heeft economische waarde en leidt tot meer transparantie en participatie. Zo kunnen anderen nieuwe toepassingen ontwikkelen en/of deze gegevens via (mobiele) applicaties laagdrempelig ontsluiten richting klanten.

#### *7. Onze gemeente hergebruikt gegevens*

Binnen de Nederlandse overheid is afgesproken dat burgers niet wordt gevraagd om gegevens waar de overheid zelf al over beschikt. In het algemeen is de beschikbaarheid en kwaliteit van gegevens belangrijk. Door duidelijke afspraken te maken over waar gegevens worden beheerd en waarvandaan ze worden verstrekt wordt het delen ervan veel eenvoudiger en worden mogelijke inconsistenties voorkomen. Op landelijk niveau zijn er hiertoe basisregistraties gedefinieerd die door alle overheidsorganisaties moeten worden gebruikt.

<sup>5</sup> <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017.html>

<sup>6</sup> <http://wetten.overheid.nl/BWBR0005252/>

<sup>7</sup> <http://wetten.overheid.nl/BWBR0011468/>

## 8. *Onze gemeente gaat op een vertrouwelijke manier met gegevens om*

Klanten verwachten dat de gemeente op een zorgvuldige manier met hun gegevens om gaat en dat deze niet in handen komen van onbevoegden. De visiebrief 'Digitale overheid 2017' besteedt daarom specifiek aandacht aan informatieveiligheid. Ontwikkelingen als consumerization en tijd- en plaatsonafhankelijk werken vragen ook om extra aandacht voor de beveiliging van informatie. Grenzen van organisaties vervagen en traditionele beveiligingsmaatregelen passen niet meer. Cybercriminaliteit kan zorgen voor ernstige ontregeling van organisaties. Het is daarom belangrijk de risico's expliciet te maken. Hierdoor kunnen de meest passende maatregelen worden genomen en worden overmatige maatregelen vermeden.

## 3.4 Soorten architecturen

In de GEMMA 2 wordt uitgegaan van drie architectuurlagen en sluit hiermee aan op de onderverdeling die de Nederlandse Overheid Referentiearchitectuur (NORA)<sup>8</sup> hanteert. Het 9-vlaks model uit de NORA wordt gebruikt als architectuurraamwerk voor het rangschikken en geordend presenteren van principes, standaarden, bouwstenen en afspraken. Het architectuurraamwerk, zoals in figuur 2 afgebeeld, bestaat uit de drie (horizontaal weergegeven) eerdergenoemde architectuurlagen (bedrijfsarchitectuur, informatiearchitectuur en technische architectuur) en drie kolommen die respectievelijk beschrijven wie, wat op welke wijze (hoe) doet. Lagen en kolommen overlappen elkaar, daardoor ontstaan er negen vlakken.

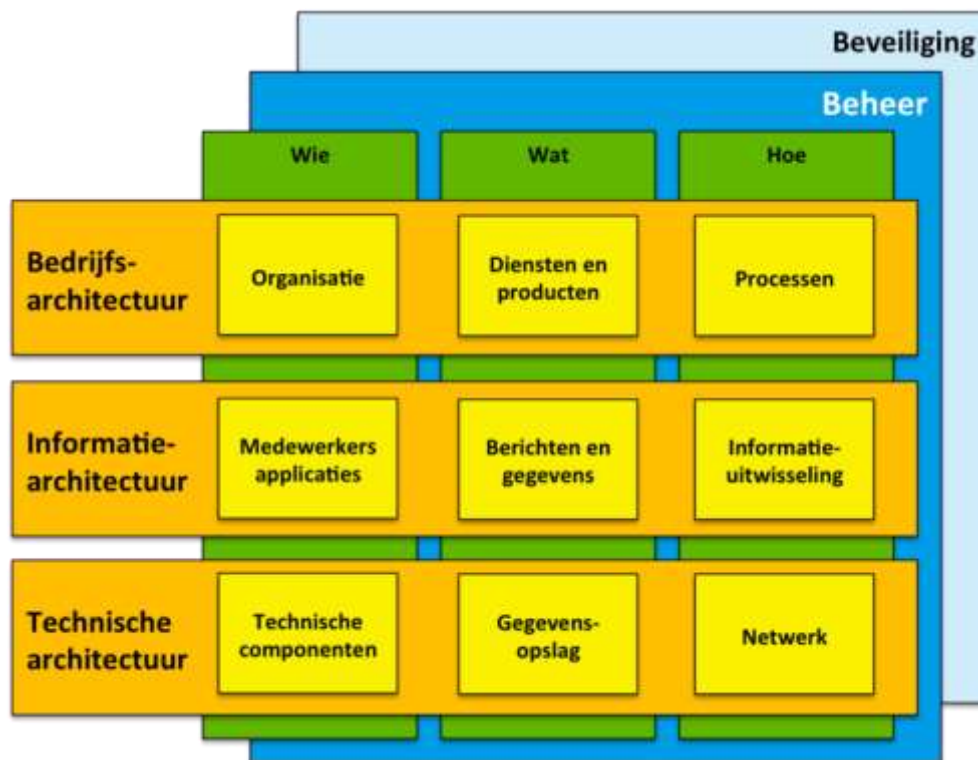
De drie architectuurlagen waar in GEMMA 2 van wordt uitgegaan zijn:

- **Business- of bedrijfsarchitectuur:** Hiermee begint iedere architectuur, deze bevat de business doelstellingen, strategie en uitwerking processen, functies en rollen.
- **Informatiearchitectuur:** Hierin wordt de informatiestrategie en de uitwerking naar concrete projecten op basis van business doelen en ontwikkelingen tot stand gebracht, bijvoorbeeld gegevens- en berichtenarchitectuur, applicatie-architectuur.
- **Technische architectuur:** Architectuur die weergeeft wat nodig is om de informatievoorziening te laten werken zoals deze is beschreven in de informatie-architectuur, bijvoorbeeld hardware en netwerk specificaties, overzicht van technische componenten en hun relatie met informatiesystemen. Deze technische architectuur is (nog) niet beschikbaar. Een goed voorbeeld van een verdieping in de vorm van beveiligingspatronen is het beveiligingskatern van de NORA waar patronen en implementatie richtlijnen worden beschreven welke gerelateerd kunnen worden aan de BIR en BIG op basis van de ISO 27002.<sup>9</sup>

In figuur 2 zijn van links naar rechts de vlakken op het niveau van de businessarchitectuur organisatie, producten en diensten en processen. Op het niveau van de informatiearchitectuur zijn deze vlakken, medewerkers en applicaties, berichten en gegevens en informatie-uitwisseling en op het niveau van de technische architectuur zijn deze vlakken, technische componenten, gegevensopslag en netwerken. Het 9-vlaks model wordt aangevuld met twee aparte vlakken voor informatiebeveiliging en beheer, die alle lagen en kolommen overstijgen.

<sup>8</sup> [http://noraonline.nl/wiki/NORA\\_online](http://noraonline.nl/wiki/NORA_online)

<sup>9</sup> <http://www.noraonline.nl/wiki/Beveiliging>



**Figuur 2 Het NORA architectuurraamwerk.**

### 3.4.1 GEMMA 2 Bedrijfsarchitectuur

De bedrijfs- of businessarchitectuur is het startpunt van iedere architectuur en dus ook van GEMMA 2.<sup>10</sup> Hieronder valt de inrichting van organisatie, producten en processen. Omdat gemeenten qua organisatie-inrichting allemaal van elkaar verschillen is het moeilijk daar in een referentiearchitectuur iets over te zeggen. Het bedrijfsfunctiemodel en objectmodel zijn ontwikkeld om generiek model neer te zetten voor diversiteit aan gemeenten. Uitgegaan van primaire processen van gemeenten.

#### *Bedrijfsfunctiemodel*

Een bedrijfsfunctiemodel is een model van de bedrijfsfuncties van een organisatie. Het beschrijft wat een organisatie doet onafhankelijk van hoe het wordt uitgevoerd. Het kijkt naar een organisatie als een verzameling van activiteiten die worden uitgevoerd en clustert deze tot logische eenheden die soortgelijke kennis en competenties vragen. Het model vormt een neutraal referentiekader waarin nog geen organisatiespecifieke keuzen staan. Bij het ontwerpen van informatievoorziening kan dit model dan ook als startpunt worden gebruikt en verder worden gedetailleerd.

<sup>10</sup> [http://www.gemmaonline.nl/index.php/GEMMA\\_Bedrijfsarchitectuur](http://www.gemmaonline.nl/index.php/GEMMA_Bedrijfsarchitectuur)



**Bedrijfsfunctiemodel**



**Figuur 3 GEMMA 2 Bedrijfsfuncties .**

## Bedrijfsobjectmodel

Een bedrijfsobjectmodel beschrijft de objecten waarmee organisaties te maken hebben. Het gaat met name over de objecten waarover ook gegevens worden vastgelegd. Het wordt ook wel een conceptueel gegevensmodel genoemd. Het is nadrukkelijk nog geen logisch gegevensmodel. Het model beschrijft de grotere eenheden van gegevens in een taal die breed in de organisatie herkenbaar is en geeft dus nog geen details over de precieze gegevensstructuur. Het legt focus op grotere verzamelingen van gestructureerde gegevens die breed worden gedeeld in de organisatie.

Het model lijkt op het bedrijfsfunctiemodel in de zin dat het ook onafhankelijk is van de inrichting van organisatie en IT en daardoor ook een stabiel referentiekader biedt. Bedrijfsfuncties zijn een clustering van activiteiten. Binnen deze activiteiten worden bepaalde gegevens gecreëerd. Voor een goede informatiehuishouding is het belangrijk dat het eigenaarschap van gegevens is belegd. Het eigenaarschap van bedrijfsfuncties en gegevens is nauw aan elkaar gerelateerd; de eigenaar van een bedrijfsfunctie (voor zover deze is benoemd) is in veel gevallen ook de logische eigenaar van de gegevens die worden gecreëerd in de bedrijfsfunctie.

## Procesarchitectuur

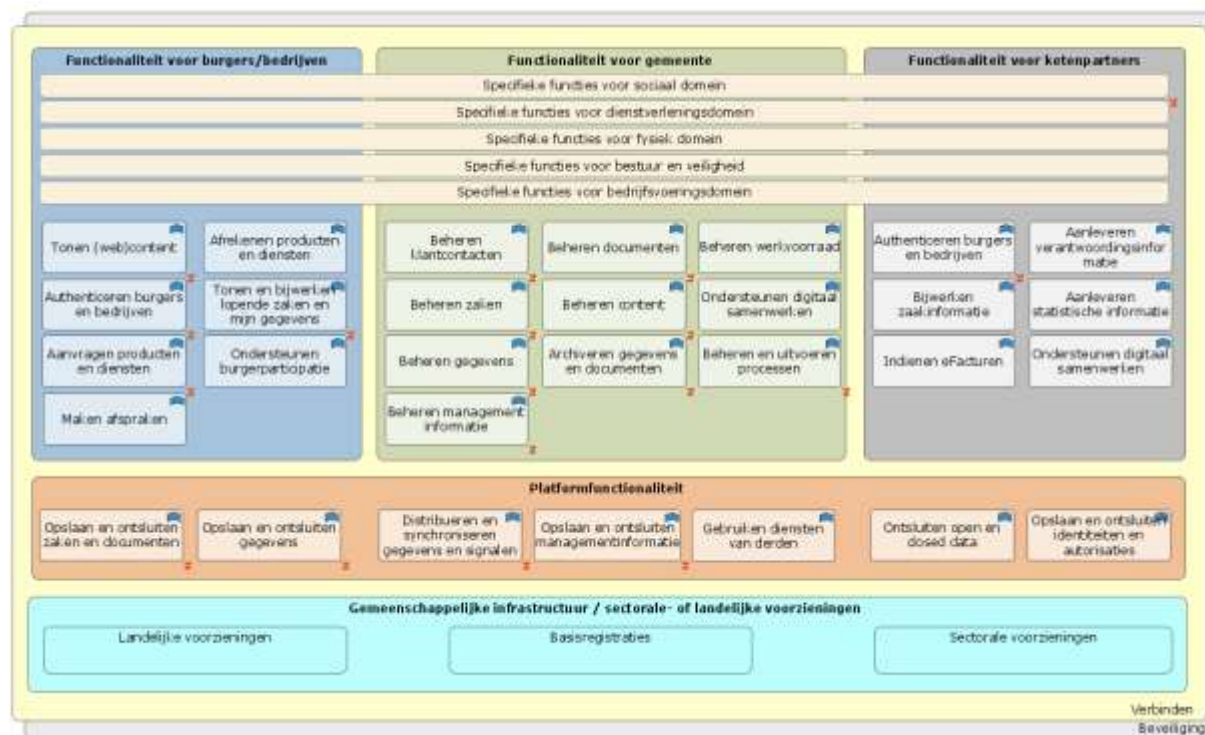
Naast de bedrijfsfuncties en bedrijfsobjecten bestaat de bedrijfsarchitectuur in GEMMA 2 nog uit de GEMMA Procesarchitectuur. Deze bevat een set richtlijnen en principes voor het kijken naar gemeentelijke processen. Daarnaast geeft het een overzicht van alle gemeentelijke bedrijfsprocessen.

## 3.4.2 GEMMA 2 Informatiearchitectuur



## Informatiearchitectuur

De GEMMA 2 informatiearchitectuur<sup>11</sup> gaat over de inrichting van de informatiehuishouding van gemeenten. De informatiehuishouding betreft de referentiecomponenten en applicatiefunctionaliteit waarmee de gegevens kunnen worden opgeslagen, geraadpleegd en processen kunnen worden ondersteund etc. Ook de informatiemodellen en berichtenstandaarden die zorgen voor een efficiënte en gestandaardiseerde manier van informatie-uitwisseling, zijn onderdeel van de informatiearchitectuur. De GEMMA 2 informatiearchitectuur schetst een integraal beeld van de gemeentelijke architectuur.



De applicatiefuncties in de GEMMA 2 informatiearchitectuur (zie figuur 5) bouwen op van beneden naar boven, van generiek naar specifiek.

- Helemaal onderaan staat de generieke gemeenschappelijke functionaliteit. Deze laag bestaat uit landelijke voorzieningen, sectorale voorzieningen of basisregistraties.
- Een laag hoger staat de GEMMA 2 Platformfunctionaliteit. Deze laag bevat functionaliteit die generiek is voor de hele gemeente en veelal ook maar één keer geïmplementeerd dient te worden. Deze platformfunctionaliteit wordt door andere applicaties gebruikt om diensten aan eindgebruikers aan te bieden.
- De laag functionaliteit voor eindgebruikers (burgers/bedrijven, gemeente en ketenpartners) beschrijft specifieke functionaliteit voor eindgebruikers. Er wordt hier een onderscheid gemaakt naar doelgroep om aan te geven dat de gemeentelijke informatievoorziening van de toekomst ten dienste staat van de hele gemeenschap.
- Binnen de functionaliteit voor eindgebruikers wordt een onderscheid gemaakt tussen generieke functionaliteit die voor alle domeinen gebruikt wordt (zoals beheren zaken) en domeinspecifieke functionaliteit(bijvoorbeeld Tonen sociale kaart).
  - Functionaliteit voor burgers/bedrijven: functionaliteit waarmee burgers of bedrijven kunnen interacteren met de gemeente.

<sup>11</sup> [http://www.gemmaonline.nl/index.php/GEMMA\\_Informatiearchitectuur](http://www.gemmaonline.nl/index.php/GEMMA_Informatiearchitectuur)

- Functionaliteit voor gemeente: functionaliteit die ambtenaren ondersteunt in de uitvoering van haar processen.
- Functionaliteit voor ketenpartners: functionaliteit voor de gemeente waardoor ketenpartners kunnen interacteren met de gemeente.
- Specifieke functionaliteit werken we per thema uit. Momenteel is dit al gedaan voor het Thema Sociaal Domein. Op deze plaat zijn de specifieke functies voor het sociaal domein getekend in relatie tot de generieke functies. Op basis van het relevante bedrijfsfunctiemodel. Overige thema's volgen.

### 3.4.3 Overige architectuurmodellen

#### Applicatiearchitectuur

Het gemeentelijk applicatielandschap bestaat nog uit veel applicaties die al dan niet aan elkaar gekoppeld zijn. Dit leidt tot een applicatielandschap met weinig onderlinge samenhang en die moeilijk aanpasbaar is. Daardoor is het moeilijk voor gemeentelijke I&A afdelingen om flexibel en snel in te spelen op de veranderende eisen die de omgeving aan de gemeentelijke organisatie en haar informatiehuishouding stelt. Om samenhang en flexibiliteit in de informatiehuishouding te creëren, is het nodig generieke functies uit de applicatie te halen en vervolgens generiek ter beschikking te stellen. Hierbij sluit GEMMA 2 aan bij het gedachtegoed van de diensten/service georiënteerde architectuur.

Daarnaast is het van belang dat applicaties voor de ondersteuning van de informatievoorziening en gemeentelijke processen deze functionaliteit met de juiste standaarden ondersteunen. De GEMMA Softwarecatalogus<sup>12</sup> is een online informatiesysteem dat het (verwachte) softwareaanbod voor gemeenten en het gebruik door gemeenten in kaart brengt. Per softwareproduct is aangegeven wat de globale functionaliteit is, wat de productplanning is en welke standaarden worden ondersteund op basis van een structuur van de GEMMA Referentiecomponenten<sup>13</sup>. Deze GEMMA referentiecomponenten worden gebruikt voor sturing op overzicht, samenhang en op realisatie van de informatievoorziening. In de actuele thema's - zoals zaakgericht werken, informatiebeveiliging of ondernemersdienstverlening - komen de referentiecomponenten terug als verbinding tussen benodigde functionaliteit en de verandering en reeds beschikbare voorzieningen.

#### Gegevens- en berichtenarchitectuur

Om de GEMMA 2 architectuurprincipes te realiseren, is standaardisatie nodig op het gebied van gegevens en berichten. Zonder een goede harmonisatie van gegevens en berichten is een effectieve uitwisseling van data tussen applicaties vrijwel onmogelijk. In de gegevens- en berichtenarchitectuur wordt nader ingegaan op de standaardisatie van informatiemodellen en berichtenstandaarden.

<sup>12</sup> <https://www.softwarecatalogus.nl/>

<sup>13</sup> [http://www.gemmaonline.nl/index.php/GEMMA\\_Applicatielandschap](http://www.gemmaonline.nl/index.php/GEMMA_Applicatielandschap)

## **4. Informatiebeveiliging in GEMMA 2**

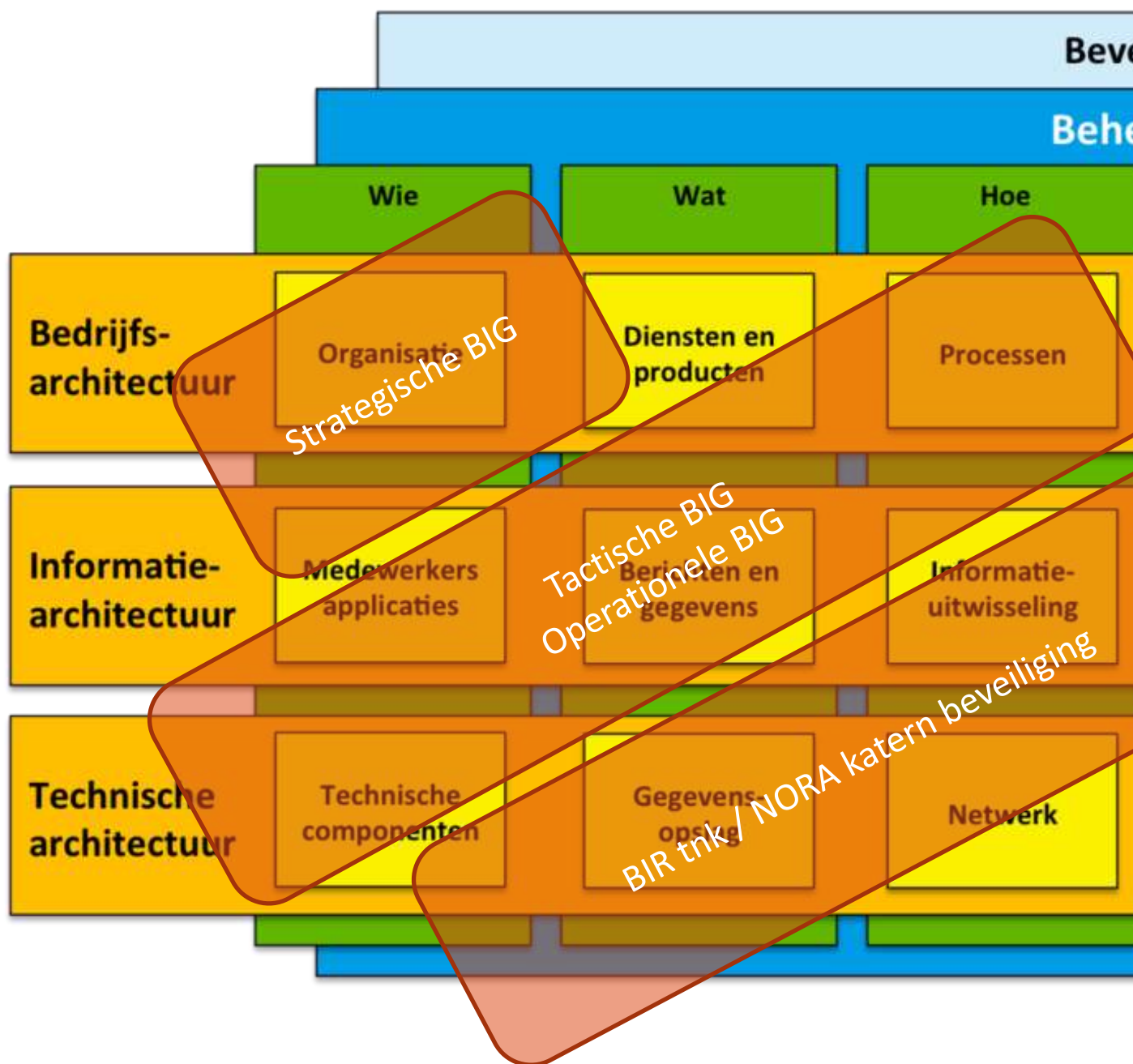
### **4.1 Inleiding**

In dit hoofdstuk gaat over de positionering van de BIG ten opzichte van de GEMMA 2.

### **4.2 Positionering informatiebeveiliging binnen GEMMA 2**

Informatiebeveiliging wordt bereikt door een geschikte verzameling beheersmaatregelen in te zetten, waaronder beleid, werkwijzen, procedures, organisatiestructuren en programmatuur- en apparatuurfuncties. Deze beheersmaatregelen moeten worden vastgesteld, gecontroleerd, beoordeeld en waar nodig verbeterd, om te waarborgen dat de specifieke beveiligings- en bedrijfsdoelstellingen van de organisatie worden bereikt. Dit behoort te worden gedaan in samenhang met andere bedrijfsbeheerprocessen.

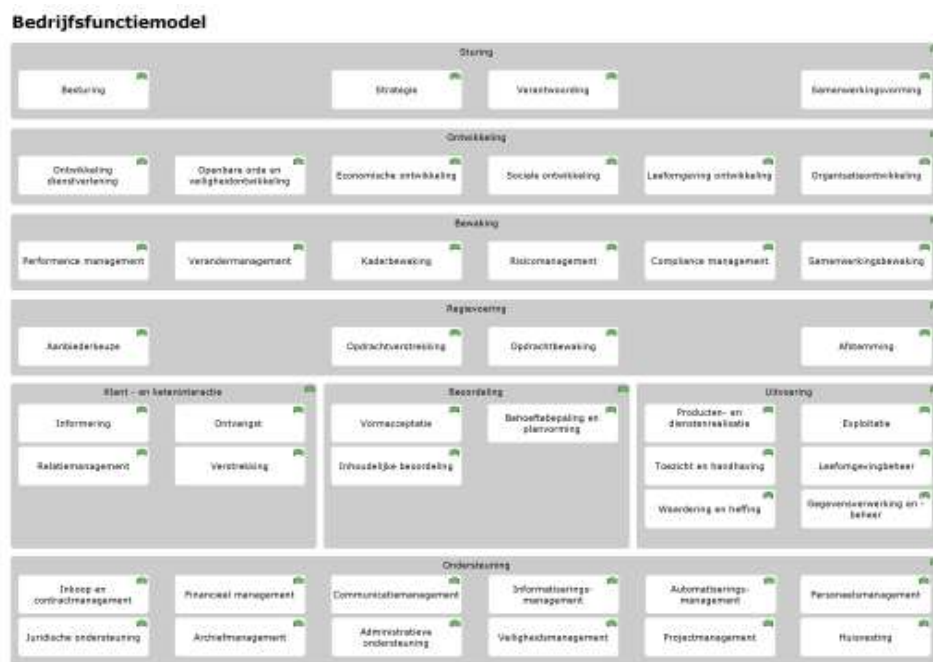
In het negenvlaks-model van de GEMMA 2 kan de BIG op hoofdlijnen worden gepositioneerd zoals in figuur 3 weergegeven. In de BIR technisch normenkader (BIR tnk) en in de NORA het beveiligingskatern worden technische architectuur patronen uitgewerkt. Om aan te geven dat er technische uitwerkingen bestaan die ook voor de Gemma gebruikt kunnen worden is dat hier genoemd. Dit document gaat niet verder in op techniek.



**Figuur 4** Negenvlak-model van de GEMMA 2 en positionering BIG delen

### 4.3 Bedrijfsarchitectuur

In deze paragraaf wordt een overzicht gegeven van de relevante aspecten van informatiebeveiliging betreffende de in de GEMMA 2 beschreven modellen. De opbouw van de paragrafen is steeds hetzelfde. Als eerste wordt aangegeven welke bedrijfsfuncties het betreft, daarna volgt een onderbouwing waarom informatiebeveiliging relevant is en als laatste worden maatregelen opgesomd die in dit kader geïmplementeerd kunnen worden.<sup>14</sup>



**Figuur 5 GEMMA 2 Bedrijfsfuncties .**

## 4.3.1 Sturing

De functie 'sturing' betreft het richting geven aan de organisatie door het bepalen van de gewenste verandering en de kaders waarbinnen deze verandering moet plaatsvinden, het vormen van samenwerkingsverbanden om hierin vulling aan te geven en het verantwoorden of doelstellingen ook behaald zijn.

- Besturing: Het inrichten en uitvoeren van de besluitvormingsprocessen en -structuren en het nemen van strategische besluiten.
- Strategie: Het bepalen welke veranderingen zouden moeten worden doorgevoerd en de doelstellingen die daaraan ten grondslag liggen.
- Verantwoording: Het rapporteren naar belanghebbenden binnen en buiten de organisatie over de waarin wordt voldaan aan verplichtingen en afspraken.
- Samenwerkingsvorming

## Informatiebeveiliging

Informatiebeveiliging is een integrale verantwoordelijkheid van het lijnmanagement. Het College van Burgemeester en Wethouders van de gemeente moet beleid vaststellen. In het beleid behoort de risicoperceptie beschreven te worden, de verdeling van verantwoordelijkheden, de structuur van de beveiligingsorganisatie, de omgang met betrouwbaarheidseisen en de naleving van wet- en regelgeving. Bij het vormen van samenwerkingsverbanden blijft de verantwoordelijkheid voor

<sup>14</sup> Op basis van 'pas toe of leg uit'.

informatiebeveiliging van het College gehandhaafd. Het College moet de samenwerking ook op het gebied van informatiebeveiliging besturen.

## **Tactische Baseline**

Uit de BIG zijn de volgende normen relevant voor de functie 'sturing':

- 5.1.1 Beleidsdocumenten voor informatiebeveiliging

Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

- 5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

- 6.1.1 Betrokkenheid van het College van B&W bij beveiliging

Het hoogste management behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

- 6.1.2 Coördineren van beveiliging

Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies.

- 6.1.3 Verantwoordelijkheden

Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.

- 6.1.6 Contact met overheidsinstanties

Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.

- 6.1.8 Beoordeling van het informatiebeveiligingsbeleid

De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging.

## **Operationele Baseline:**

In de operationele baseline is voor de gemeenten een voorbeeld beleidsdocument opgenomen

## **4.3.2 Ontwikkeling**

De functie Ontwikkeling geeft verdere invulling aan een gewenste verandering op de inhoudelijke beleidsterreinen van de gemeente, zoals leefomgeving en openbare orde en veiligheid, en de ontwikkeling van de dienstverlening en de eigen organisatie. Het behelst het opstellen van de gewenste portfolio van producten en diensten alsook het verder uitwerken van deze producten en diensten voor de verschillende beleidsterreinen van de gemeente.

## **Informatiebeveiliging**

Voor het ontwikkelen van nieuwe producten en diensten waarin informatie wordt verwerkt, dient een gemeente ervoor zorg te dragen dat deze voldoen aan het informatiebeveiligingsbeleid en aan de betrouwbaarheidseisen die aan de producten en diensten moeten worden gesteld. Deze eisen kunnen worden bepaald middels een baselinetoets, een PIA en eventueel een diepgaande risicoanalyse.

Bij aanschaf van producten dient een proces gevolgd te worden waarbij beveiliging een onderdeel is van het gevraagde informatiesysteem (BIG h.12) en de sturing op externe partijen (BIG h. 6).

Als het een informatiesysteem is dat door een leverancier wordt ontwikkeld, kan de gemeente eisen dat tijdens de ontwikkeling gebruik dient te worden gemaakt van de methode 'Grip op secure software development (SSD)'.<sup>15</sup> Deze methode beschrijft hoe de gemeente (opdrachtgever) grip krijgt op het ontwikkelen van goed beveiligde software. De beveiligingseisen die de gemeente (opdrachtgever) kan hanteren als eisen aan de op te leveren software, zijn beschreven in het document Grip op SSD: SIVA Beveiligingseisen.<sup>16</sup>

Betreffende de functies voor het ontwikkelen van (organisatie)veranderingen en het ontwikkelen van de dienstverlening, kunnen ook de beveiligingsorganisatie (BIG h. 6) waaronder het beschrijven van rollen en verantwoordelijkheden, personele beveiliging (BIG h. 8) en logische en fysieke toegang (BIG h. 9 en h. 11) bij organisatieveranderingen van belang.

## Tactische baseline

### H. 6 Doelstelling

Het beveiligen van de informatie en ICT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

- 6.2.1 Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

- 6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij

In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen.

### H. 12 Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

- 12.1.1 Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

## Operationele baseline

- Baselinetoets BIG
- Diepgaande Risicoanalysemethode gemeenten
- Privacy Impact Assessment (PIA)
- Procedure nieuwe ICT-voorzieningen
- Handreiking proces wijzigingsbeheer
- Handleiding projectkaart risicoanalyse informatiebeveiliging<sup>17</sup>
- Inkoopvoorwaarden

### 4.3.3. Bewaking

De functie 'bewaking' controleert of binnen alle overige bedrijfsfuncties aan de gewenste doelstellingen en randvoorwaarden wordt voldaan. Indien nodig worden van de juiste corrigerende maatregelen genomen. Bewaking beschrijft deze controle vanuit een zestal perspectieven: performance management, verandermanagement, kaderbewaking, risicomanagement, compliance

<sup>15</sup> <http://www.cip-overheid.nl/wp-content/uploads/2014/05/Grip-op-SSD-Het-proces-v1-03.pdf>

<sup>16</sup> <http://www.cip-overheid.nl/wp-content/uploads/2014/05/Grip-op-SSD-SIVA-Beveiligingseisen-v1-0.pdf>

<sup>17</sup> Op het moment van schrijven is dit BIG-OP document nog in ontwikkeling.



management en samenwerkingsbewaking. Voor alle zes functies is ten minste het informatiebeveiligingsbeleid van de gemeente van toepassing. Overige relevante beveiligingsthema's zouden beveiligingsorganisatie (verandermanagement en samenwerkingsbewaking), toegangsbeveiliging en naleving (verandermanagement en kaderbewaking), en beheer en ontwikkeling (performance management) kunnen zijn. De specifieke verbinding met informatiebeveiliging is afhankelijk van de invulling van de functies.

Risicomanagement en compliance management zijn belangrijke onderwerpen voor informatiebeveiliging. Risicomanagement is het systematisch bepalen, bewaken en beheren van de risico's waaraan de organisatie wordt blootgesteld. Als risico's betrekking hebben op informatie, is risico-inschatting en risicobeheersing voor passende informatiebeveiliging noodzakelijk. Informatiebeveiliging is een belangrijk onderwerp binnen risicomanagement voor gemeenten. Dit is eveneens het geval voor compliance management. Compliance management is het bewaken of processen worden uitgevoerd in lijn met geldende wet- en regelgeving. Voor compliance op het gebied van informatiebeveiliging is onder meer de Wbp en het door de gemeenten zelfopgelegde normenkader van de BIG van toepassing.

Een belangrijke nieuwe verplichting voor gemeenten en andere organisaties is de toevoeging van een meldplicht voor inbreuken op de beveiligingsmaatregelen voor persoonsgegevens aan de Wbp. Met deze meldplicht datalekken wil de regering de gevolgen van een datalek voor de betrokkenen zoveel mogelijk beperken en hiermee een bijdrage leveren aan het behoud en herstel van vertrouwen in de omgang met persoonsgegevens. Met dit voorstel moet de verantwoordelijke bij een datalek, waarbij kans is op verlies of onrechtmatige verwerking van persoonsgegevens, niet alleen tijdig een melding doen bij de toezichthouder, de Autoriteit Persoonsgegevens<sup>18</sup>, maar ook de betrokkene informeren. Als er geen tijdige melding wordt gemaakt van een datalek kan dit bestraft worden met een bestuurlijk boete.

## Risicomanagement

### Tactische baseline:

- 5.1.1 Beleidsdocumenten voor informatiebeveiliging

Informatiebeveiligingsbeleid behoort door het hoogste management te worden goedgekeurd en gepubliceerd. Het document dient tevens kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen.

1. Er is een beleid voor informatiebeveiliging door het College van Burgemeester en Wethouders vastgesteld, gepubliceerd en beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

- 6.2.1 Identificatie van risico's die betrekking hebben op externe partijen

De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.

- 6.2.2 Beveiliging beoordelen in de omgang met klanten

Alle geïdentificeerde beveiligingseisen behoren te worden beoordeeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.

- 12.2.3 Integriteit van berichten

Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

- 12.1.1 Analyse en specificatie van beveiligingseisen

<sup>18</sup> De Autoriteit Persoonsgegevens is het voormalige College Beschermingspersoonsgegevens (CBP).



In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

## Operationele Baseline

- Baselinetoets BIG
- Diepgaande Risicoanalysemethode gemeenten
- Privacy Impact Assessment (PIA)

## Compliance management

Tactische Baseline:

- 15.1.3 Bescherming van bedrijfsdocumenten  
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
- 15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens  
De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving (zoals Wet bescherming persoonsgegevens (Wbp)<sup>19</sup> en Archiefwet<sup>20</sup>), voorschriften en indien van toepassing contractuele bepalingen.

### 4.3.4 Regievoering

Regievoering is het kiezen en aansturen van partners die werk uitvoeren namens de gemeente. Denk bijvoorbeeld aan zorgaanbieders. Het gaat over het coördineren van de kwaliteit en de levering van uitbestede diensten door aanbieders. Regievoering bestaat vier onderdelen:

- Aanbiederkeuze: Het kiezen van een aanbieder voor een bepaalde in te kopen dienst.
- Opdrachtverstrekking: Het verstrekken van een opdracht aan een aanbieder voor het leveren van een dienst.
- Opdrachtbewaking: Het bewaken of de door een aanbieder geleverde dienst conform afspraken is.
- Afstemming: Het inhoudelijke en procesmatig afstemmen met een partij met wie wordt samengewerkt of waarvan diensten worden betrokken, zodat beiden over de juiste informatie beschikken.

Veel gemeentelijke informatie wordt door derden beheerd of verwerkt. Gemeenten hebben bijvoorbeeld informatieverwerkende processen uitbesteed of zetten informatiesystemen van derden in om (delen van) processen uit te voeren. Om controle te houden op de risico's gerelateerd aan informatie is het essentieel om regie te houden op het verwerven en bewaken van uitbestede diensten. Het uitgangspunt bij uitbesteding is dat de gemeente te allen tijde verantwoordelijk blijft voor de informatiebeveiliging.

Verschillende hoofdstukken uit de BIG zijn van toepassing op uitbestede diensten. Het informatiebeveiligingsbeleid van de gemeente moet de omgang met uitbesteedde diensten en betrouwbaarheidseisen beschrijven (BIG h. 5). In de beveiligingsorganisatie is een verantwoordelijke aangesteld voor de uitbesteedde dienst (BIG h. 6) en in paragraaf 6.2 wordt apart de handhaving beschreven van de beveiliging van (informatie)systemen die door externe partijen worden beheerd.

<sup>19</sup> <http://wetten.overheid.nl/BWBR0011468/>

<sup>20</sup> <http://wetten.overheid.nl/BWBR0007376/>

## 4.3.5 Klant - en keteninteractie

De functie klant- en keteninteractie betekent het aangaan van de interactie met de klant en ketenpartners, het ervoor zorgen dat zij over de juiste gegevens en informatie beschikken en het ontvangen meldingen, verzoeken en gegevens.

- Informering: Het geven van algemene of persoonlijke informatie of advies.
- Ontvangst: Het ontvangen van signalen, gegevens of een verzoek of een melding die aanleiding geeft om een proces te starten of die anderszins bijdraagt aan de uitvoering van het proces.
- Relatiemanagement: Het onderhouden van de relatie met klanten en ketenpartners.
- Verstrekking: Het verstrekken van gegevens of een ander resultaat van een proces aan een klant of ketenpartner.

Bij het uitwisselen van informatie met klanten en ketenpartners dienen gemeenten een overzicht te hebben van welke algemene of persoonlijke informatie, adviezen en inlichtingen mogen worden verstrekt aan klanten en ketenpartners. Vastgesteld moet worden welke informatie mag en moet worden gedeeld met klanten en ketenpartners. Bij het verstrekken van (persoons)gegevens dient altijd de wet- en regelgeving in acht te worden genomen, conform de bedrijfsfunctie compliance management. Om te waarborgen dat de juiste informatie wordt gedeeld, dient de gemeente passende maatregelen te nemen. De BIG kent een standaard set aan maatregelen die gaan over het uitwisselen van informatie. Vaststellen of boven het basisbeveiligingsniveau van de BIG nog extra maatregelen noodzakelijk zijn, is afhankelijk van het belang en het gewenste beveiligingsniveau van de informatie. De mogelijke schade die een dreiging (bijv. misbruik door oneigenlijke toegang) kan toebrengen aan bepaalde informatie(documenten) en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Het management dient vervolgens aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt. Dit identificeren en mitigeren van risico's maakt tevens onderdeel uit van de bedrijfsfunctie risicomanagement.

### Tactische Baseline:

- 10.8.1 Beleid en procedures voor informatie-uitwisseling  
Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- 10.8.2 Uitwisselingsovereenkomsten  
Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- 10.8.4 Elektronisch berichtenuitwisseling  
Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.
- 10.8.5 Systemen voor bedrijfsinformatie  
Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

### Operationele Baseline:

- Baselinetoets BIG
- Diepgaande Risicoanalysemethode gemeenten
- Privacy Impact Assessment (PIA)

- Bewerkersovereenkomst
- Handreiking beveiligingsparagraaf SLA
- Encryptie beleid (PKI)
- Logische toegangsbeveiliging

## 4.3.6 Beoordeling

Het inhoudelijk beoordelen van een melding of verzoek.

- Behoeftebepaling en planvorming

Het in kaart brengen van de behoeften van een klant en eventuele betrokkenen en het opstellen van een plan voor de ondersteuning van de klant.

- Inhoudelijke beoordeling

Het inhoudelijk bestuderen en analyseren van een verzoek of melding en het nemen van een besluit over de verdere afhandeling.

- Vormacceptatie

Het bepalen of een verzoek of melding voldoet aan de formele indieningsvereisten.

Voor het beoordelen van een melding of een verzoek is het waarborgen van diverse aspecten van informatiebeveiliging van belang. Om de juiste beschikbaarheid te waarborgen, dient bijvoorbeeld de beschikbaarheid van systemen voldoende te zijn om wettelijke termijnen te kunnen behalen en change- en patchmanagement goed zijn ingericht om onbeschikbaarheid bij systeemwijzigingen te voorkomen. Ten aanzien van de inhoudelijke beoordeling is onder meer de integriteit van de informatie belangrijk. Deze dient conform het gewenste betrouwbaarheidsniveau te worden geborgd. Ook de vertrouwelijkheid van de gegevensverwerking voor beoordelingen moet worden gewaarborgd. Belangrijke beveiligingsonderwerpen voor de vertrouwelijkheid zijn onder meer toegangsbeveiliging (BIG h. 11), het vastleggen en naleven van verantwoordelijkheden van medewerkers ten aanzien van beveiliging (BIG h. 9 en h. 15) en het correct verwerken van gegevens in systemen en applicaties (BIG h. 12.2).

### Tactische baseline

H.11 Beheersen van de toegang tot informatie.

12.2 Correcte verwerking in toepassingen

Doelstelling

Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.6 Beheer van technische kwetsbaarheden

Doelstelling

Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.

## 4.3.7 Uitvoering

De bedrijfsfunctie uitvoering is de daadwerkelijke levering van producten en diensten waar een klant om heeft gevraagd of die anderzijds tot de verantwoordelijkheid van de gemeente behoren.

- Exploitatie

Het conform privaatrechtelijke grondslag exploiteren van de gemeentelijke voorzieningen zoals een zwembad, museum, parkeergarage of sportaccommodatie.

- Gegevensverwerking en -beheer

Het geheel van activiteiten om in de gemeente op het juiste moment over de juiste gegevens van de juiste kwaliteit te beschikken

- Leefomgevingbeheer

het in stand houden van de gemeentelijke openbare ruimte door het plegen van onderhoud, het inzamelen van zwerfafval en reiniging.

- Producten- en dienstenrealisatie.

Het uitvoeren van activiteiten om producten en diensten te leveren.

- Toezicht en handhaving

Het ervoor zorgen dat vastgestelde regelgeving wordt nageleefd.

- Waardering en heffing

Het vaststellen en opleggen van de aanslag voor gemeentelijke belastingen en heffingen.

Tot de uitvoering behoren een veelvoud aan activiteiten waarbij informatie en daarmee informatiebeveiliging een rol speelt. Door de breedte van de bedrijfsfunctie zullen vrijwel alle onderdelen van de BIG behandeld moeten worden.

## 4.3.8 Ondersteuning

De bedrijfsfunctie ondersteuning zorgt ervoor dat de juiste mensen en middelen beschikbaar zijn zodat de overige functies uitgevoerd kunnen worden. De betrouwbaarheidseisen van de informatiebeveiliging voor de bedrijfsfunctie ondersteuning worden in veel gevallen worden bepaald door de processen die worden ondersteund. De automatisering moet bijvoorbeeld systemen kunnen leveren die voldoen aan de eisen van de verantwoordelijke. Hetzelfde geldt voor de veiligheidsmanagement: de eisen aan de fysieke beveiliging worden bepaald door de verantwoordelijke, die

- Archiefmanagement: Het ervoor zorgdragen dat gegevens beschikbaar blijven zodat het handelen van gemeenten publiek verantwoord kan worden.
- Automatiseringsmanagement: Het ervoor zorgen dat IT-systemen beschikbaar zijn voor de ondersteuning van de informatievoorziening.
- Huisvesting: De interne verlening van vastgoeddiensten, parkeerdiensten en nutsdiensten (gas, water en licht) en de planning daarvan en het onderhoud daarop.
- Informatiseringsmanagement: Het ervoor zorgen dat informatiebehoeften bekend zijn en zijn vertaald naar gewenste functionaliteiten van de informatievoorziening.
- Inkoop en contractmanagement: Het verwerven van middelen en het bewaken van de afspraken hierover met de leverancier.
- Juridische ondersteuning: Het bieden van advies en ondersteuning op het gebied van wet- en regelgeving.
- Personeelsmanagement: Het ervoor zorgdragen dat er competente medewerkers beschikbaar zijn voor de uitvoering van bedrijfsprocessen.
- Projectmanagement: Het ervoor zorgdragen dat projecten beheerst worden uitgevoerd.
- Veiligheidsmanagement: Het bewaken dat de organisatie voldoet aan alle aspecten van veiligheid en beveiliging.

## 4.4 Procesarchitectuur

De GEMMA Procesarchitectuur 2.0 wil gemeenten ondersteunen bij het invoeren van procesgericht werken en procesmanagement. Dit ondersteunen gebeurt op twee terreinen:

1. Denken: het aanreiken van een referentiekader voor gemeentelijke processen, procesarchitectuur en procesmanagement;

2. Doen: het bieden van handreikingen en praktijkvoorbeelden om gemeenten te ondersteunen bij de invoering van procesgericht werken.

Een goed overzicht van en een goede grip op de gemeentelijke processen helpt de complexiteit reduceren en de efficiëntie verhogen. De procesarchitectuur bevat een set richtlijnen en principes voor het kijken naar gemeentelijke processen. Daarnaast geeft het een overzicht van alle gemeentelijke bedrijfsprocessen.

De procesarchitectuur kan met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden verbonden door te focussen op de verbeterprocessen beschreven in de BIG. Een essentieel onderdeel in de BIG is, net als in de ISO 27001, een *Information Security Management System*. Dit is een set van beleidsmaatregelen voor beveiliging die middels een *plan, do, check en act* (PDCA)-cyclus moeten worden uitgevoerd in een gemeente. De PDCA-stappen in een ISMS zijn als volgt:

Plan: het ontwikkelen en vaststellen van het ISMS

Do: implementeren en uitvoeren van het ISMS

Check: Monitoren en toetsen van het ISMS

Act: Onderhouden en verbeteren van het ISMS.

Het ontwikkelen en uitvoeren van een ISMS is beschreven in hoofdstuk 5 en 6 van de BIG. In die hoofdstukken is onder meer de noodzakelijkheid van het inventariseren van risico's, het periodiek vaststellen van informatiebeveiligingsbeleid en het toewijzen van rollen en verantwoordelijkheden terug te vinden.

In de procesarchitectuur vormen de primaire bedrijfsprocessen samen met de sturende bedrijfsprocessen een PDCA (Plan-Do-Check-Act)-cyclus. De cyclus wordt als volgt ingevuld:

- Plan: wordt ingevuld door het *programmeren*;
- Do: wordt ingevuld door de primaire bedrijfsprocessen;
- Check: is het *evalueren*;
- Act: is het *vormen van de strategie*; hieronder valt ook het bijstellen hiervan.





*Procesarchitectuur 2.0*

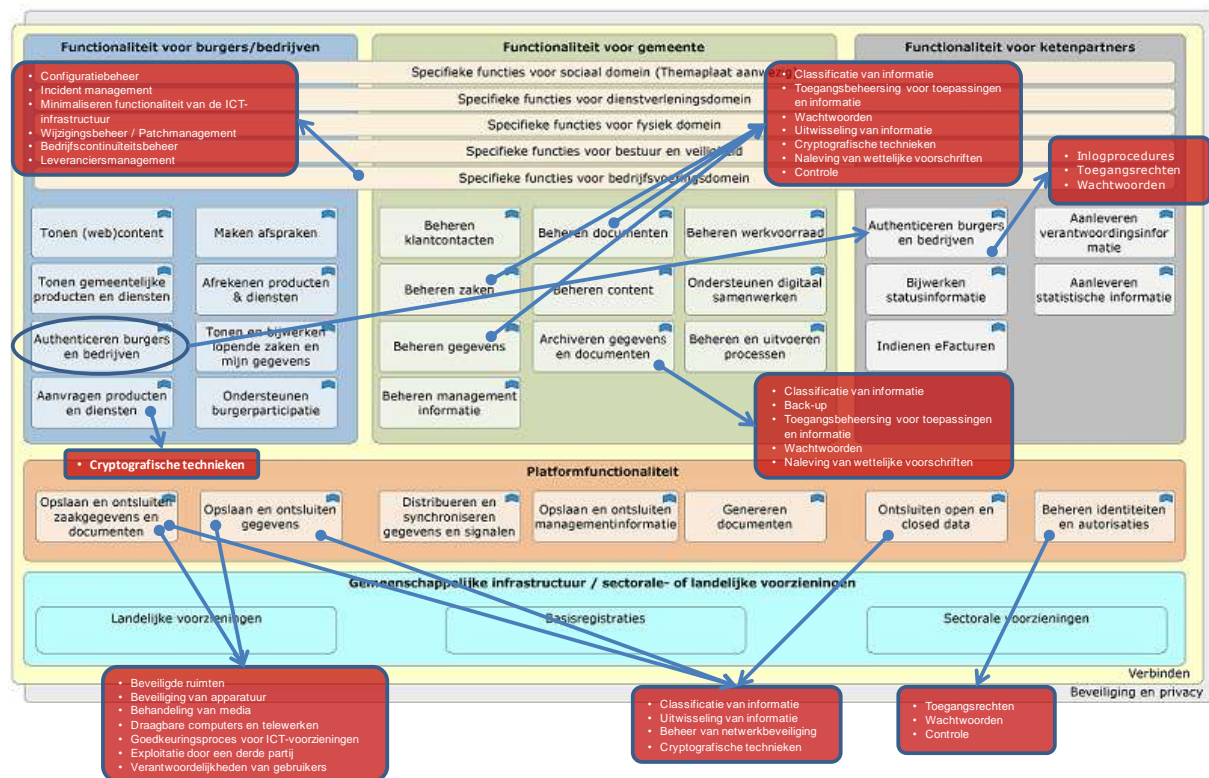
## **4.5 Informatiearchitectuur**

De GEMMA 2 informatiearchitectuur (zie figuur 8) gaat over de inrichting van de informatiehuishouding van gemeenten. De informatiehuishouding betreft de referentiecomponenten en applicatiefunctionaliteit waarmee de gegevens kunnen worden opgeslagen, geraadpleegd en processen kunnen worden ondersteund. Ook de informatiemodellen en berichtenstandaarden die zorgen voor een efficiënte en gestandaardiseerde manier van informatie-uitwisseling, zijn onderdeel van de informatiearchitectuur.

### *Informatiearchitectuur en informatiebeveiliging*

Voor de informatiearchitectuur van GEMMA 2 zijn verschillende aspecten van informatiebeveiliging relevant. Het opslaan, raadplegen en beschikbaar stellen van informatie dient zorgvuldig plaats te vinden zodat bijvoorbeeld privacy van burgers is gewaarborgd, maar gevoelige gegevens en processen van de gemeente integer en beschikbaar zijn. In het algemeen moet de werking van de informatiearchitectuur voldoen aan het gemeentelijke informatiebeveiligingsbeleid, geldende wet- en regelgeving, eisen voor landelijke voorzieningen en basisregistraties. Belangrijke beveiligingsthema's zoals toegangsbeveiliging, dataclassificatie en backup van gegevens moeten worden ingericht.

Voor de vanuit informatiebeveiligingsperspectief belangrijkste applicatiefuncties of groep met specifieke functies worden in de volgende paragrafen de relevante informatiebeveiligingsaspecten weergegeven. Figuur 7 geeft hiervan een totaaloverzicht.



**Figuur 6 GEMMA 2 informatiearchitectuur en belangrijkste informatiebeveiligingsaspecten**

## 4.5.1 Functionaliteit voor burgers/bedrijven

### Aanvragen producten en diensten (Applicatiefunctie)

Functionaliteit die burgers of bedrijven in staat stelt om producten of diensten aan te vragen. Bijvoorbeeld een (intelligente) formulierentoe passing.

#### Informatiebeveiliging: veilig communiceren met de overheid

De Nederlandse overheid stelt steeds meer diensten en informatie beschikbaar via internet. Zo is het mogelijk om bij (een aantal) gemeenten, bijvoorbeeld een uittreksel uit het geboorteregister of een vergunning aan te vragen via hun website. Maar hoe weet je nu zeker dat de website waar je je gegevens invult daadwerkelijk van je gemeente is en of de communicatie met een overheidswebsite beveiligd is, zodat deze gegevens niet 'op straat' komen te liggen? Een oplossing hiervoor zijn zogenaemde SSL-certificaten. Een certificaat voegt een uniek zegel toe aan een website.

#### Tactische Baseline

Relevante informatiebeveiligingsaspecten m.b.t. het aanvragen van producten of diensten zijn:

##### Cryptografische technieken

Informatie m.b.t. cryptografische technieken is te vinden in:

- Tactische Baseline: 12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen  
Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.



- Tactische Baseline: 15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen  
Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

## Operationele Baseline

- Operationele Baseline: Encryptiebeleid (PKI)

## Authenticeren burgers en bedrijven (Applicatiefunctie)

Functionaliteit waarmee burgers of bedrijven zich kunnen identificeren en authenticeren voor de geboden diensten. Deze applicatiefunctie bestaat uit de volgende subfuncties:

- Authenticeren burgers: Functionaliteit voor het **authenticeren van burgers** (bij voorkeur geleverd door DigID).
- Authenticeren bedrijven: Functionaliteit voor het **authenticeren van bedrijven** (bij voorkeur door eHerkenning).

*Informatiebeveiliging: Waarborgen vertrouwelijkheid en integriteit gemeentelijke informatievoorziening*

Logische toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform ontsloten en beschikbaar gesteld wordt, bijvoorbeeld Basisregistratie Personen (BRP)<sup>21</sup> en Suwinet<sup>22</sup>. Alle gebruikers van gemeentelijke informatiesystemen dienen, volgens logische toegangsbeveiliging procedures, geautoriseerd te worden.

Relevante informatiebeveiligingsaspecten m.b.t. authenticeren burgers en bedrijven zijn:

### Inlogprocedures

Informatie m.b.t. inlogprocedures is te vinden in:

- Tactische Baseline: 11.5.1 Beveiligde inlogprocedures  
Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

### Toegangsbeheersing voor toepassingen en informatie

Informatie m.b.t. toegangsbeheersing voor toepassingen en informatie is te vinden in:

- Tactische Baseline: 11.5.2 Gebruikersidentificatie en -authenticatie  
Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
- Tactische Baseline: 11.6.1 Beperken van toegang tot informatie  
Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid. Denk hierbij aan de volgende beveiligingsmaatregelen:

<sup>21</sup> De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen.

<sup>22</sup> Suwinet is het informatiesysteem van gegevensuitwisseling op het terrein van werk en inkomen



11.6.1.1. In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.

11.6.1.3. Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

- Tactische Baseline: 11.6.2 Isoleren van gevoelige systemen  
Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben. Denk hierbij aan de volgende beveiligingsmaatregelen:  
11.6.2.1. Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.
- Operationele Baseline: Beleid logische toegangsbeveiliging

## Wachtwoorden

Informatie m.b.t. wachtwoorden is te vinden in:

- Tactische Baseline 11.5.3 Systemen voor wachtwoordenbeheer  
Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
- Operationele Baseline: Wachtwoordbeleid

Technieken en tools die authenticeren burgers en bedrijven kunnen ondersteunen zijn:

- Identity & Access Management (IAM)

## 4.5.2 Functionaliteit voor gemeente

### Archiveren gegevens en documenten (Applicatiefunctie)

Functionaliteit voor het archiveren van gegevens en documenten. Hieronder valt functionaliteit voor het converteren van documenten naar archiefformaat en het beheren van gearchiveerde documenten en dossiers.

#### *Informatiebeveiliging: waarborgen beschikbaarheid gegevens en documenten*

Er dient rekening mee gehouden te worden dat in principe van alle data en applicaties back-ups gemaakt moeten worden. Echter er kan een verschil zijn per systeem. Bijvoorbeeld in de gevoeligheid van de gegevens, de belangrijkheid van het proces of de soort data. Daarnaast zijn er ook back-ups nodig van de machine (server) instellingen, de zogenaamde system

In principe is een back-up geen digitaal archief. Dat wil zeggen dat de bewaartermijn van back-ups bepaald wordt door de rotatie van de back-upmedia of tapes. Back-up media die versleten zijn, of niet meer gebruikt worden, moeten vernietigd worden conform het beleid voor behandeling van digitale media.

Een back-up van een digitaal archief, als er een digitaal archief is en de originele stukken zijn vernietigd (substitutie), krijgen back-up tapes van dat archief mogelijk dezelfde status als de reproducties in het archiefsysteem. Deze tapes dienen langer bewaard en gelezen te kunnen worden. Afhankelijk van de soort data gelden dus andere bewaartermijnen. Waarbij soms ook de apparatuur om de media te kunnen lezen in stand moet worden gehouden.

Logische toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen

deze gemeentelijke informatiesystemen. Dit blijft uiteraard ook gelden voor gegevens en documenten die zijn gearhiveerd, als informatie niet bestemd is voor iedereen dan dient dit gehandhaafd te blijven in het zakenmagazijn maar ook in de archief situatie, tenzij de informatie eigenaar declassificeert of minder gevoelig maakt

## **Tactische Baseline**

Relevante informatiebeveiligingsaspecten m.b.t. authenticeren burgers en bedrijven zijn:

### **Classificatie van informatie**

Informatie m.b.t. classificatie van informatie is te vinden in:

- Tactische Baseline 7.2.1 Richtlijnen voor classificatie van informatie  
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Tactische Baseline 7.2.2 Labeling en verwerking van informatie  
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

### **Operationele baseline**

- Operationele Baseline: Handreiking Dataclassificatie

## **Back-up**

Informatie m.b.t. back-ups is te vinden in:

- Tactische Baseline: 10.5.1 Reservekopieën maken (back-ups)  
Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.
- Operationele Baseline: Back-up en Recovery Gemeente

## **Toegangsrechten**

Informatie m.b.t. toegangsrechten is te vinden in:

- Tactische Baseline: 11.5.2 Gebruikersidentificatie en -authenticatie  
Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
- Operationele Baseline: Beleid logische toegangsbeveiliging

## **Wachtwoorden**

Informatie m.b.t. wachtwoorden is te vinden in:

- Tactische Baseline 11.5.3 Systemen voor wachtwoordenbeheer  
Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
- Operationele Baseline: Wachtwoordbeleid

## **Naleving van wettelijke voorschriften**

- Tactische Baseline: 15.1.3 Bescherming van bedrijfsdocumenten  
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
- Tactische Baseline: 15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving (zoals Wet bescherming persoonsgegevens (Wbp)<sup>23</sup> en Archiefwet<sup>24</sup>), voorschriften en indien van toepassing contractuele bepalingen.

Operationele Baseline: Baselinetoets BIG

Operationele Baseline: Diepgaande Risicoanalysemethode gemeenten

Operationele Baseline: Privacy Impact Assessment (PIA)

## Beheren documenten (Applicatiefunctie)

Functionaliteit voor het beheren van documenten. Hieronder valt het aanmaken, bijwerken en verwijderen van documenten, alsmede functionaliteit voor het digitaliseren, metadateren en ondertekenen van documenten. De applicatiefunctie 'beheren documenten' bestaat uit de volgende subfuncties:

- Metadateren documenten: Functionaliteit voor het **toevoegen van metadata aan documenten/informatieobjecten**. Bijvoorbeeld auteur, aanmaakdatum of onderwerp.
- Digitaliseren documenten: Functionaliteit voor het **digitaliseren van papieren documenten**. Functionaliteit om papieren documenten te scannen (digital-reborn), eventueel verder te digitaliseren (tekstherkenning) en in een digitaal formaat op te slaan.
- Tonen en bijwerken documenten: Functionaliteit voor het **tonen van opgeslagen documenten** op basis van zoekparameters en functionaliteit voor het **bijwerken van deze documenten** of de bijbehorende metadata.
- Digitaal ondertekenen documenten: Functionaliteit voor het **digitaal ondertekenen van documenten en andere informatieobjecten**. Hiermee kan de echtheid en oorspronkelijkheid van de informatie worden vastgelegd en aangetoond.

*Informatiebeveiliging: Vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie*

De mogelijke schade die een dreiging (bijv. misbruik door oneigenlijke toegang) kan toebrengen aan bepaalde informatie(documenten) en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Het management dient vervolgens aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt. Het gebruik van standaard risicoanalyse hulpmiddelen is vaak een tijdrovend en abstract traject. De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie(systemen) en is daarmee een basis voor een risicoanalyse. Na de classificatie kunnen de juiste maatregelen getroffen worden waardoor enerzijds inbreuken op de veiligheid worden voorkomen en anderzijds daarvoor niet nodeloos veel inspanning getroost wordt.

Een van de maatregelen om het belang van informatie te beveiligen wordt geboden door logische toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform ontsloten en beschikbaar gesteld wordt, bijvoorbeeld Basisregistratie Personen (BRP)<sup>25</sup> en Suwinet<sup>26</sup>. Alle gebruikers van gemeentelijke informatiesystemen dienen, volgens logische toegangsbeveiliging procedures, geautoriseerd te worden.

<sup>23</sup> <http://wetten.overheid.nl/BWBR0011468/>

<sup>24</sup> <http://wetten.overheid.nl/BWBR0007376/>

<sup>25</sup> De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen.

<sup>26</sup> Suwinet is het informatiesysteem van gegevensuitwisseling op het terrein van werk en inkomen

Een maatregel die de echtheid en oorspronkelijkheid van de informatie kan waarborgen is de cryptografische techniek 'digitale handtekening'. Zoals de naam al doet vermoeden, is de digitale handtekening analoog aan een gewone, met de hand gezette, handtekening. Het doel van een met de hand gezette handtekening is authenticatie van de ondertekenaar, een mogelijkheid tot verificatie hiervan door de ontvanger, en de handtekening kan tevens worden gebruikt om onweerlegbaarheid (non-repudiation) en echtheid (integriteit) te garanderen.

Relevante informatiebeveiligingsaspecten m.b.t. het beheren van documenten zijn:

## **Classificatie van informatie**

Informatie m.b.t. classificatie van informatie is te vinden in:

- Tactische Baseline 7.2.1 Richtlijnen voor classificatie van informatie  
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Tactische Baseline 7.2.2 Labeling en verwerking van informatie  
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.
- Operationele Baseline: Handreiking Dataclassificatie

## **Toegangsbeheersing voor toepassingen en informatie**

Informatie m.b.t. toegangsbeheersing voor toepassingen en informatie is te vinden in:

- Tactische Baseline: 11.5.2 Gebruikersidentificatie en -authenticatie  
Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
- Tactische Baseline: 11.6.1 Beperken van toegang tot informatie  
Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid. Denk hierbij aan de volgende beveiligingsmaatregelen:
  - 11.6.1.1. In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
  - 11.6.1.3. Bij extern gebruik vanuit een onvertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.
- Tactische Baseline: 11.6.2 Isoleren van gevoelige systemen  
Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben. Denk hierbij aan de volgende beveiligingsmaatregelen:
  - 11.6.2.1. Gevoelige systemen (met hoge beschikbaarheid of grote vertrouwelijkheid) behoren een eigen vast toegewezen (geïsoleerde) computeromgeving te hebben. Isoleren kan worden bereikt door fysieke of logische methoden.
- Operationele Baseline: Beleid logische toegangsbeveiliging

## **Wachtwoorden**

Informatie m.b.t. wachtwoorden is te vinden in:

- Tactische Baseline: 11.3.1 Gebruik van wachtwoorden  
Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.
- Operationele Baseline: Wachtwoordbeleid

## **Uitwisseling van informatie**

- Tactische Baseline: 10.8.5 Systemen voor bedrijfsinformatie  
Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

## Cryptografische technieken

Informatie m.b.t. cryptografische technieken is te vinden in:

- Tactische Baseline: 12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen  
Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
- Tactische Baseline: 15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen  
Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.
- Operationele Baseline: Encryptiebeleid (PKI)

## Controle

Informatie m.b.t. controle is te vinden in:

- Tactische Baseline: 10.10.1 Aanmaken audit-logbestanden  
Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
- Tactische Baseline: 10.10.2 Controle van systeemgebruik  
Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
- Tactische Baseline: 15.2.2 Controle op technische naleving  
Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.
- Operationele Baseline: Aanwijzing Logging

## Naleving van wettelijke voorschriften

- Tactische Baseline: 15.1.3 Bescherming van bedrijfsdocumenten  
Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
- Tactische Baseline: 15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens  
De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving (zoals Wet bescherming persoonsgegevens (Wbp)<sup>27</sup> en Archiefwet<sup>28</sup>), voorschriften en indien van toepassing contractuele bepalingen.

Operationele Baseline: Baselinetoets BIG

Operationele Baseline: Diepgaande Risicoanalysemethode gemeenten

Operationele Baseline: Privacy Impact Assessment (PIA)

Technieken en tools die beheren documenten kunnen ondersteunen zijn:

<sup>27</sup> <http://wetten.overheid.nl/BWBR0011468/>

<sup>28</sup> <http://wetten.overheid.nl/BWBR0007376/>

- Loggingsopslag
- Eventlogging
- Security Information and Event Management systeem (SIEM)

## Beheren gegevens (Applicatiefunctie)

Functionaliteit voor het **tonen en bijwerken van basis, kern, geometrische en sectorale gegevens**.

- Tonen en bijwerken geometrische gegevens: Functionaliteit voor het tonen en bijwerken van geometrische gegevens. De applicatiefunctie 'beheren gegevens' bestaat uit de volgende subfuncties:
- Tonen en bijwerken basisgegevens: Functionaliteit voor het inzien en bijwerken van basisgegevens
- Tonen en bijwerken kerngegevens: Functionaliteit voor het inzien en bijwerken van kerngegevens.
- Tonen en bijwerken sectorale (keten)gegevens: Functionaliteit voor het inzien en bijwerken van sectorale (keten) gegevens.
- Beheren terugmeldingen: Functionaliteit voor het enerzijds melden van gereede twijfel over gegevens aan de desbetreffende bronhouders en anderzijds functionaliteit voor het tonen en verwerken van de binnengekomen terugmeldingen voor registraties waarvan de gemeente de bronhouder is.

*Informatiebeveiliging: vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie*

Voor het vaststellen van het belang en het bijbehorende beveiligingsniveau van basis, kern, geometrische en sectorale gegevens met betrekking tot het beheren van deze gegevens wordt verwezen naar de applicatiefunctie 'Beheren documenten' (zie paragraaf 0).

## Beheren identiteiten en autorisaties (Applicatiefunctie)

Functionaliteit ten dienste van applicaties voor het beheren van identiteiten, rollen en autorisaties van gebruikers. Deze applicatiefunctie 'beheren identiteiten en autorisaties' bestaat uit de volgende subfunctie:

- Identity management (referentiecomponent): **De centrale opslagplaats voor het administreren van de identiteiten en rechten** van gebruikers van IT- en informatiesystemen.

*Informatiebeveiliging: Waarborgen vertrouwelijkheid en integriteit gemeentelijke informatievoorziening*

Het beheren van identiteiten en autorisaties is een belangrijke pijler van de gemeentelijke informatiebeveiliging en de gemeentelijke ICT-infrastructuur. Het regelt namelijk de kernvraagstukken "Wie ben je?" en "Wat mag je?" van het elektronische dienstverleningsproces.

Het geheel bestaat uit een verzameling, bij voorkeur generieke, voorzieningen voor het beheer en de controle van identiteiten en autorisaties van gebruikers van geautomatiseerde informatiesystemen/-diensten binnen de gemeente. De uiteindelijke functie is, dat bij het elektronisch verlenen van (informatie)diensten kan worden gecontroleerd of een persoon, die toegang vraagt tot (een deel van) de dienst, bekend is en geautoriseerd is om die toegang te verkrijgen.

Relevante informatiebeveiligingsaspecten m.b.t. het beheren van identiteiten en autorisaties zijn:

## **Toegangsrechten**

Informatie m.b.t. toegangsrechten is te vinden in:

- Tactische Baseline: 8.3.1 Beëindiging van verantwoordelijkheden  
De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen. Denk hierbij aan de volgende beveiligingsmaatregelen:
  - 8.3.1.2. Het lijnmanagement heeft een procedure vastgesteld voor beëindiging van dienstverband, contract of overeenkomst waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten, innemen van bedrijfsmiddelen en welke verplichtingen ook na beëindiging van het dienstverband blijven gelden.
  - 8.3.1.3. Het lijnmanagement heeft een procedure vastgesteld voor verandering van functie binnen de organisatie, waarin minimaal aandacht besteed wordt aan het intrekken van toegangsrechten en innemen van bedrijfsmiddelen die niet meer nodig zijn na het beëindigen van de oude functie.
- Tactische Baseline: 8.3.3 Blokkering van toegangsrechten  
De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en ICT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.
- Tactische Baseline: 11.2.1 Registratie van gebruikers  
Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
- Tactische Baseline: 11.2.2 Beheer van (speciale) bevoegdheden  
De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
- Tactische Baseline: 11.2.4 Beoordeling van toegangsrechten van gebruikers  
Het management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.
- Tactische Baseline: 11.5.2 Gebruikersidentificatie en -authenticatie  
Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
- Operationele Baseline: Beleid logische toegangsbeveiliging

## **Wachtwoorden**

Informatie m.b.t. wachtwoorden is te vinden in:

- Tactische Baseline: 11.2.3 Beheer van gebruikerswachtwoorden  
De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
- Tactische Baseline: 11.5.3 Systemen voor wachtwoordenbeheer  
Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
- Operationele Baseline: Wachtwoordbeleid

## **Controle**

Informatie m.b.t. controle is te vinden in:

- Tactische Baseline: 10.10.1 Aanmaken audit-logbestanden  
Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een

overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

- Tactische Baseline: 10.10.2 Controle van systeemgebruik  
Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
- Tactische Baseline: 10.10.3 Bescherming van informatie in logbestanden  
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
- Tactische Baseline: 10.10.4 Logbestanden van administrators en operators  
Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.
- Tactische Baseline: 10.10.5 Registratie van storingen  
Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.
- Tactische Baseline: 10.10.6 Synchronisatie van systeemklokken  
De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.
- Tactische Baseline: 10.2.2 Controle en beoordeling van dienstverlening door een derde partij  
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
- Operationele Baseline: Aanwijzing Logging

Technieken en tools die beheren identiteiten en autorisaties kunnen ondersteunen zijn:

- Identity & Access Management (IAM)
- Loggingsopslag
- Eventlogging
- Security Information and Event Management systeem (SIEM)

## Beheren zaken (Applicatiefunctie)

Functionaliteit voor het aanmaken van zaken, het tonen en bijwerken van zaakgegevens en bijbehorende documenten alsmede het agenderen van zaken en het tonen en bijwerken van zaaktypen.

### Vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie

Voor het vaststellen van het belang en het bijbehorende beveiligingsniveau van zaakgegevens en bijbehorende documenten met betrekking tot het beheren van deze gegevens wordt verwezen naar de applicatiefunctie 'Beheren documenten' (zie paragraaf 0).

## 4.5.3 Platformfunctionaliteit

### Opslaan en ontsluiten zaakgegevens en documenten (Applicatiefunctie)

Functionaliteit voor het **opslaan en aan applicaties beschikbaar stellen van zaakgegevens, zaaktypen en documenten**. Deze applicatiefunctie levert zowel diensten aan de specifieke functionaliteit van de gemeente (beheren zaken, inzage in lopende zaken voor de professional) als



aan de functionaliteit voor de burger (tonen en bijwerken lopende zaken). Deze applicatiefunctie 'Opslaan en ontsluiten zaakgegevens en documenten' bestaat uit de volgende subfuncties:

- Opslaan en ontsluiten documenten: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van al dan niet bij een zaak horende documenten.
- Opslaan en ontsluiten zaaktypen: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van zaaktypegegevens.
- Opslaan en ontsluiten zaakgegevens: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van zaakgegevens.

### **Vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie**

Voor het vaststellen van het belang en het bijbehorende beveiligingsniveau van zaakgegevens, zaaktypen en documenten met betrekking tot het ontsluiten van deze gegevens wordt verwezen naar de applicatiefunctie 'Ontsluiten open en closed data' (zie paragraaf 0).

### **Waarborgen vertrouwelijkheid en integriteit van gegevens**

Voor het opslaan van zaakgegevens, zaaktypen en documenten wordt verwezen naar de applicatiefunctie 'Opslaan en ontsluiten gegevens' (zie paragraaf 0).

## **Opslaan en ontsluiten gegevens (Applicatiefunctie)**

Functionaliteit voor het **opslaan en naar applicaties ontsluiten van basis, kern, sectorale en geometrische gegevens**. Ook het opslaan en ontsluiten van terugmeldingen valt hieronder. Deze applicatiefunctie 'Opslaan en ontsluiten gegevens' bestaat uit de volgende subfuncties:

- Opslaan en ontsluiten terugmeldingen: Functionaliteit voor het opslaan en ontsluiten van ontvangen terugmeldingen (bij gerede twijfel aan de juistheid van (authentieke) gegevens waarvoor de gemeente bronhouder is).
- Opslaan en ontsluiten basisgegevens: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van basisgegevens.
- Opslaan en ontsluiten kerngegevens: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van kerngegevens.
- Opslaan en ontsluiten geometrische gegevens: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van geometrische gegevens.
- Opslaan en ontsluiten sectorale gegevens: Functionaliteit voor het opslaan en naar andere applicaties ontsluiten van sectorale gegevens.

### **Vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie**

Voor het vaststellen van het belang en het bijbehorende beveiligingsniveau van basis, kern, sectorale en geometrische gegevens met betrekking tot het ontsluiten van deze gegevens wordt verwezen naar de applicatiefunctie 'Ontsluiten open en closed data' (zie paragraaf 0).

Voor het opslaan van basis, kern, sectorale en geometrische gegevens gelden de volgende aanvullingen.

### **Waarborgen vertrouwelijkheid en integriteit van gegevens**

Om de vertrouwelijkheid en integriteit van gegevens te waarborgen is het van belang dat wordt voorkomen dat onbevoegden toegang krijgen tot ruimtes met informatie waar zij geen kennis van behoren te nemen dan wel dat informatie kan worden aangepast. Op het moment dat ICT-voorzieningen vervangen dienen te worden is het van belang dat daar een goedkeuringsprocedure voor wordt gevolgd. De goedkeuringsprocedure dient zorg te dragen dat wijzigingen op de ICT-

infrastructuur (ICT-middelen en -diensten) efficiënt en effectief worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen die hieraan zijn gesteld.

Er is een toename van het gebruik van mobiele gegevensdragers zoals smartphones, tablets en laptops binnen de gemeenten, het is dan ook van belang dat mobiele gegevensdragers, media, draagbare computers afdoende worden beveiligd. Mobiele gegevensdragers worden gebruikt voor de transport van informatie. Vroeger gebeurde dat voornamelijk met floppy disks, tegenwoordig gebeurt dat met geheugenkaartjes, USB-sticks en bijvoorbeeld mobiele apparaten. De vormen van mobiele gegevensdragers nemen toe en daarmee ook de kans op verlies van gegevens. Daarnaast kunnen mobiele media ook een bron zijn van ongewenste software zoals virussen. Het maakt hierbij niet uit of het een gemeentelijk mobiel apparaat of een eigen mobiel apparaat (in het geval van Bring Your Own Device (BYOD)), immers op mobiele apparaten kan in meer of mindere mate data van de gemeente staan. Los van het feit of het mobiele apparaat fysiek kan zoekraken, de data is in beide gevallen van de gemeente. Daarnaast wordt er ook door gemeenten nagedacht over "het nieuwe werken" waarbij ook steeds meer gebruik gemaakt wordt van laptops.

Op het moment dat gebruik wordt gemaakt van een derde partij (bijvoorbeeld cloud) dient er te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij. De gemeente dient hiervoor wel de beveiligingseisen kenbaar te maken.

Relevante informatiebeveiligingsaspecten m.b.t. het opslaan en ontsluiten gegevens zijn:

## **Beveiligde ruimten**

- Tactische Baseline: 9.1.1 Fysieke beveiliging van de omgeving  
Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden.
- Operationele Baseline: Toegangsbeleid

## **Beveiliging van apparatuur**

- Tactische Baseline: 9.2.6 Veilig verwijderen of hergebruiken van apparatuur  
Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.
- Operationele Baseline: Encryptiebeleid (PKI)

## **Behandeling van media**

- Tactische Baseline: 10.7.1 Beheer van verwijderbare media  
Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.
- Tactische Baseline: 10.7.2 Verwijdering van media  
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
- Tactische Baseline: 10.7.3 Procedures voor de behandeling van informatie  
Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.
- Operationele Baseline: Mobiele gegevensdragers
- Operationele Baseline: Veilige afvoer van ICT-middelen
- Operationele Baseline: Encryptiebeleid (PKI)

## **Draagbare computers en telewerken**

- Tactische Baseline: 11.7.1 Draagbare computers en communicatievoorzieningen  
Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
- Tactische Baseline: 11.7.2 Telewerken  
Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.
- Operationele Baseline: Mobile Device Management
- Operationele Baseline: Telewerkbeleid

## **Goedkeuringsproces voor ICT-voorzieningen**

- Tactische Baseline: 6.1.4 Goedkeuringsproces voor ICT-voorzieningen  
Er behoort een goedkeuringsproces voor nieuwe ICT-voorzieningen te worden vastgesteld en geïmplementeerd.
- Operationele Baseline: Procedure nieuwe ICT-voorzieningen

## **Exploitatie door een derde partij**

- Tactische Baseline: 10.2.1 'Dienstverlening'  
Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
- Tactische Baseline: 10.2.2 'Controle en beoordeling van dienstverlening door een derde partij'  
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
- Tactische Baseline: 10.2.3 'Beheer van wijzigingen in dienstverlening door een derde partij'  
Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.
- Operationele Baseline: Contractmanagement
- Operationele Baseline: Inkoopvoorwaarden en informatiebeveiligingseisen
- Operationele Baseline: Bewerksvereenkomst
- Operationele Baseline: Handreiking Service Level Agreements
- Operationele Baseline: Cloud Computing

## **Verantwoordelijkheden van gebruikers**

- Tactische Baseline: 11.3.2 Onbeheerde gebruikersapparatuur  
Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.
- Tactische Baseline: 11.3.3 Clear desk en clear screen  
Er behoort een clear desk-beleid voor papier en verwijderbare opslagmedia en een clear screen-beleid voor ICT-voorzieningen te worden ingesteld.
- Operationele Baseline: Handreiking communicatieplan informatiebeveiliging

Technieken en tools die beheren identiteiten en autorisaties kunnen ondersteunen zijn:

- Mobile Device Management

## Ontsluiten open en closed data (Applicatiefunctie)

Functionaliteit waarmee open data en (sectorale) closed data worden **ontsloten naar het publiek en/of belanghebbenden**. Open data is een term die wordt gebruikt om vrij beschikbare informatie te duiden en closed data is een term die gebruikt wordt om gegevens mee te duiden die alleen gedeeld mogen worden met partijen die daar doelbinding voor hebben. Deze applicatiefunctie 'Ontsluiten open en closed data' bestaat uit de volgende subfunctie:

- Gemeentelijke servicebus (referentiecomponent): Systeem waarmee koppelingen tussen gemeentelijk systemen gerealiseerd worden. Een gemeentelijke servicebus is in de basis een generieke Enterprise Service Bus (ESB) waarmee gemeente specifieke koppelingen worden gerealiseerd. Een ESB biedt minimaal functionaliteit voor het versturen en beheren van elektronische berichten. Tevens kan een ESB services aanbieden voor het routeren, transformeren en eventueel orchestreren van het berichtenverkeer. De component die deze services aanbiedt, wordt ook een Integratie server of een broker genoemd.

## Vaststellen belang en bijbehorende beveiligingsniveau van gemeentelijke informatie

De mogelijke schade die een dreiging (bijv. misbruik door oneigenlijke toegang) kan toebrengen aan bepaalde informatie(documenten) en de kans dat het optreedt, kan met een risicoanalyse worden geëvalueerd. Het management dient vervolgens aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt. Het gebruik van standaard risicoanalyse hulpmiddelen is vaak een tijdrovend en abstract traject. De voorgestelde classificatiemethodiek geeft een snelle indicatie van het belang van de informatie(systemen) en is daarmee een basis voor een risicoanalyse. Na de classificatie kunnen de juiste maatregelen getroffen worden waardoor enerzijds inbreuken op de veiligheid worden voorkomen en anderzijds daarvoor niet nodeloos veel inspanning getroost wordt.

Een van de maatregelen om het belang van (closed) informatie te beveiligen wordt geboden door logische toegangsbeveiliging vormt een belangrijk aspect van de gemeentelijke informatiebeveiliging. Logische toegangsbeveiliging zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze gemeentelijke informatiesystemen. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform ontsloten en beschikbaar gesteld wordt, bijvoorbeeld Basisregistratie Personen (BRP)<sup>29</sup> en Suwinet<sup>30</sup>. Alle gebruikers van gemeentelijke informatiesystemen dienen, volgens logische toegangsbeveiliging procedures, geautoriseerd te worden.

Versleuteling (encryptie) is een manier om gegevens te beveiligen door ze onleesbaar te maken voor onbevoegden. Dit doe je als informatie niet voor iedereen bestemd is. Hierdoor kun je je beschermen tegen bijvoorbeeld afluisteren (sniffing) en maak je een man-in-the-middle aanval moeilijker. Versleuteling van berichten kan worden gebruikt:

- Om berichten onleesbaar te maken voor anderen, of;
- Om te controleren of een bericht inderdaad van een bepaalde afzender afkomstig is.

Bij het uitbesteden van de verwerking van persoonsgegevens worden door de Wet bescherming persoonsgegevens (Wbp) nadere eisen gesteld. De verantwoordelijke<sup>31</sup> (in dit geval de gemeente) dient een schriftelijke overeenkomst af te sluiten met de bewerker<sup>32</sup> (in dit geval de derde partij), deze overeenkomst heet de bewerkersovereenkomst.

<sup>29</sup> De Basisregistratie Personen (BRP) heeft de Gemeentelijke Basisadministratie Personen (GBA) vervangen.

<sup>30</sup> Suwinet is het informatiesysteem van gegevensuitwisseling op het terrein van werk en inkomen

<sup>31</sup> De verantwoordelijke is volgens de Wet bescherming persoonsgegevens (Wbp) degene die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt (Art. 1 sub d Wbp).

<sup>32</sup> De Wbp definieert de bewerker als 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen' (Art. 1 sub e Wbp).

Relevante informatiebeveiligingsaspecten m.b.t. het ontsluiten open en closed data zijn:

## **Classificatie van informatie**

Informatie m.b.t. classificatie van informatie is te vinden in:

- Tactische Baseline 7.2.1 Richtlijnen voor classificatie van informatie  
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
- Tactische Baseline 7.2.2 Labeling en verwerking van informatie  
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.
- Operationele Baseline: Handreiking Dataclassificatie

## **Uitwisseling van informatie**

- Tactische Baseline: 10.8.1 Beleid en procedures voor informatie-uitwisseling  
Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
- Tactische Baseline: 10.8.2 Uitwisselingsovereenkomsten  
Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
- Tactische Baseline: 10.8.4 Elektronisch berichtenuitwisseling  
Informatie die een rol speelt bij elektronische berichtenuitwisseling behoort op geschikte wijze te worden beschermd.
- Tactische Baseline: 10.8.5 Systemen voor bedrijfsinformatie  
Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.
- Operationele Baseline: Bewerkersovereenkomst

## **Beheer van netwerkbeveiliging**

- Tactische Baseline: 10.6.1 Maatregelen voor netwerken  
Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

## **Cryptografische technieken**

Informatie m.b.t. cryptografische technieken is te vinden in:

- Tactische Baseline: 12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen  
Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
- Tactische Baseline: 15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen  
Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.
- Operationele Baseline: Encryptiebeleid (PKI)

## **Specifieke functies voor bedrijfsvoeringsdomein (Groep)**

Applicatiefuncties specifiek voor de ondersteunende functies. Bijvoorbeeld personeelszaken, gebouwenbeheer of een configuratie-database.

## **Beheren van ICT-infrastructuur en -diensten**

Er dient zorg voor worden gedragen dat de gegevens over de ICT-infrastructuur (ICT-middelen en -diensten) betrouwbaar worden vastgelegd en dat actuele en relevante gegevens aan andere ICT-beheerprocessen worden geleverd over de ICT-middelen, hun onderlinge samenhang (relaties) en de relaties met de ICT-diensten (configuratiebeheer). Indien deze gegevens niet juist, volledig en tijdig worden geïdentificeerd en vastgelegd, bestaat het risico dat de hiervan afhankelijke ICT-beheerprocessen niet van juiste en volledige informatie worden voorzien, waardoor zowel de beschikbaarheid, integriteit, vertrouwelijkheid als controleerbaarheid van de ICT-diensten kan worden aangetast. De procedures waarborgen dat alle wijzigingen in de configuraties juist, volledig en tijdig worden vastgelegd in de registratie. Configuratiebeheer is voorwaarden-scheppend voor bijna alle andere ICT-beheerprocessen.

Beveiligingsincidenten (security events) op een computer of computernetwerk, maar ook verdachte activiteiten door het personeel dienen adequaat gedetecteerd, gemeld en behandeld te worden om daarmee de kans op uitval van bedrijfsvoeringsprocessen of schade ontstaan als gevolg van het incident te minimaliseren, dan wel te voorkomen. Dit is zo belangrijk omdat 100% beveiligen niet bestaat en los daarvan: incidenten zijn niet te voorkomen. Het is niet de vraag óf er iets gaat gebeuren maar wanneer. De belangrijkste te verwachte incidenten kunnen van te voren bedacht worden en de bijpassende reactie en escalatie procedure kan dus ook van te voren uitgewerkt en geoefend worden. Incidenten staan vaak niet op zichzelf en kunnen een uitwerking hebben naar andere ketenpartners. Sommige incidenten doen zich niet bij één gemeente voor maar bij meerdere. Een incident moet behalve intern opgelost soms ook extern geëscaleerd worden zodat er anderen gewaarschuwd kunnen worden en daarmee de impact van het incident zo klein als mogelijk gehouden kan worden.

Eén van de makkelijkste doelen voor een aanval is een niet goed actueel gehouden systeem met de laatste patches en updates en een systeem waarbij functionaliteiten en privileges niet zijn teruggebracht tot het minimum dat noodzakelijk is voor het uitvoeren van de taak (hardening). De overbodige functies in besturingssystemen dienen uitgeschakeld te worden en/of van het systeem verwijderd te worden. Tevens dienen zodanige waarden toegekend te worden aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat.

Wijzigingen op de ICT-infrastructuur (ICT-middelen en -diensten) dienen zo efficiënt en effectief te worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit van de dienstverlening, zodat deze dienstverlening blijft voldoen aan de eisen die hieraan zijn gesteld (wijzigingsbeheer). Hiervoor dienen wijzigingen te worden geautoriseerd met inachtneming van de risico's voor de ICT-diensten, tijdig en volledig te worden doorgevoerd en te worden beoordeeld op doeltreffendheid. Dit alles resulteert in het feit dat de kans op het niet beschikbaar zijn van de ICT-dienstverlening als gevolg van wijzigingen afneemt, en dat eventuele toch opgetreden storingen korter duren. Tevens draagt het zorg dat uit beveiligingsoogpunt relevante instellingen van de ICT-infrastructuur niet ongecontroleerd en ongeautoriseerd gewijzigd kunnen worden. De ICT-infrastructuur, die aan de beveiligingsnormen voldoet, blijft aan het afgesproken niveau voldoen. In het verlengde hiervan dienen patches op gecontroleerde beheerste (risico beperkende) wijze uitgerold te worden. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware.

Ook dienen er maatregelen genomen te worden die onderbreking van bedrijfsactiviteiten tegengaan, kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen

in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen (Bedrijfscontinuïteitsbeheer).

Op het moment dat gebruik wordt gemaakt van een derde partij (bijvoorbeeld cloud) dient er te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij. De gemeente dient hiervoor wel de beveiligingseisen kenbaar te maken.

Relevante informatiebeveiligingsaspecten m.b.t. specifieke functies voor het bedrijfsvoeringsdomein zijn:

## **Configuratiebeheer**

- Tactische Baseline: 7.1.1 Inventarisatie van bedrijfsmiddelen  
Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.
- Tactische Baseline: 7.1.2 Eigendom van bedrijfsmiddelen  
Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.
- Tactische Baseline: 12.4.1 Beheersing van operationele programmatuur  
Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.
- Operationele Baseline: Samenhang beheerprocessen en informatiebeveiliging
- Operationele Baseline: Handreiking proces configuratiebeheer

## **Incident management**

- Tactische Baseline: 13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen  
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
- Tactische Baseline: 13.1.2 Rapportage van zwakke plekken in de beveiliging  
Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en – diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.
- Tactische Baseline: 13.2.1 Verantwoordelijkheden en procedures  
Er behoren verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.
- Tactische Baseline: 13.2.2 Leren van informatiebeveiligingsincidenten  
Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.
- Tactische Baseline: 13.2.3 Verzamelen van bewijsmateriaal  
Waar een vervolprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
- Operationele Baseline: Samenhang beheerprocessen en informatiebeveiliging
- Operationele Baseline: Incidentmanagement en responsebeleid

## **Minimaliseren functionaliteit van de ICT-infrastructuur**

- Tactische Baseline: 10.4.2 Maatregelen tegen 'mobile code'



Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

- Tactische Baseline: 10.6.1 Maatregelen voor netwerken  
Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.
- Tactische Baseline: 11.4.4 Bescherming op afstand van poorten voor diagnose en configuraties  
De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
- Tactische Baseline: 11.4.5 Scheiding van netwerken  
Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
- Tactische Baseline: 12.4.1 Beheersing van operationele programmatuur  
Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.
- Operationele Baseline: Samenhang beheerprocessen en informatiebeveiliging
- Operationele Baseline: Hardening beleid

## **Wijzigingsbeheer / Patchmanagement**

- Tactische Baseline: 6.1.4 Goedkeuringsproces voor ICT-voorzieningen  
Er behoort een goedkeuringsproces voor nieuwe ICT-voorzieningen te worden vastgesteld en geïmplementeerd.
- Tactische Baseline: 10.1.2 Wijzigingsbeheer  
Wijzigingen in ICT-voorzieningen en informatiesystemen behoren te worden beheerst.
- Tactische Baseline: 12.5.1 Procedures voor wijzigingsbeheer  
De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.
- Tactische Baseline: 12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem  
Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.
- Tactische Baseline: 12.5.3 Restricties op wijzigingen in programmatuurpakketten  
Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.
- Tactische Baseline: 12.6.1 Beheersing van technische kwetsbaarheden  
Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.
- Operationele Baseline: Samenhang beheerprocessen en informatiebeveiliging
- Operationele Baseline: Procedure nieuwe ICT-voorzieningen
- Operationele Baseline: Handreiking proces wijzigingsbeheer
- Operationele Baseline: Patchmanagement voor gemeenten

## **Bedrijfscontinuïteitsbeheer**

- Tactische Baseline: 14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer



Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

- Tactische Baseline: 14.1.2 Bedrijfscontinuïteit en risicobeoordeling  
Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.
- Tactische Baseline: 14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging  
Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.
- Tactische Baseline: 14.1.4 Kader voor de bedrijfscontinuïteitsplanning  
Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.
- Tactische Baseline: 14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen  
Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en ge-update, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

## **Operationele Baseline**

Samenhang beheerprocessen en informatiebeveiliging

## **Leveranciersmanagement**

- Tactische Baseline: 6.2.1 Identificatie van risico's die betrekking hebben op externe partijen  
De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.
- Tactische Baseline: 6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij  
In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen.
- Tactische Baseline: 10.2.1 'Dienstverlening'  
Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
- Tactische Baseline: 10.2.2 'Controle en beoordeling van dienstverlening door een derde partij'  
De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
- Tactische Baseline: 10.2.3 'Beheer van wijzigingen in dienstverlening door een derde partij'  
Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.
- Tactische Baseline: 10.8.2 Uitwisselingsovereenkomsten

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

- Operationele Baseline: Contractmanagement
- Operationele Baseline: Inkoopvoorwaarden en informatiebeveiligingseisen
- Operationele Baseline: Bewerkersovereenkomst
- Operationele Baseline: Handreiking Service Level Agreements
- Operationele Baseline: Operationele Baseline: Cloud Computing

Technieken en tools die beheren identiteiten en autorisaties kunnen ondersteunen zijn:

- Configuratiebeheerdatabase (CMDB)
- Servicedesk tool
- Incidentenregistratiesysteem
- Wijzigingsregistratiesysteem

